NAVAL POSTGRADUATE SCHOOL

Monterey, California

THESIS

PRIORITIZATION OF INFORMATION ASSURANCE (IA) TECHNOLOGY IN A RESOURCE CONSTRAINED ENVIRONMENT

By

Carl Phillip Brodhun III

December 2001

Thesis Advisors:	Cynthia E. Irvine
	Raymond R. Buettner
Associate Thesis Advisor	William J. Haga

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December, 2001	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE: Prioritization of Information Assurance (IA) Technology in a Resource Constrained Environment	**5. FUNDING NUMBERS**
6. AUTHOR(S): Carl Phillip. Brodhun III	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT ***(maximum 200 words)***

Classical risk analysis is a static process that does not account for rapid evolutionary or generational changes in technology and technological solutions. This thesis defines a process that expands classical risk analysis to *increase visualization* of the secuurity environment of an information system. It provides a *comparative analysis* of system attributes and encourages*focused communications* between decision-makers and information systems technicians.

Personal interviews with domain experts from four organizations were used to construct a baseline model. Face validity of the model was determined during sessions with the domain experts. The model was calibrated to two specific scenarios using a pair of surveys to set link values and establish data for the initial nodes. A verification phase compared rough results from the model with expert opinion.

The model *evaluated, prioritized and graphically illustrated* shortfalls within two information systems based on the relative importance of specific criteria established by the domain experts. It facilitated the extraction of implicit or tacit knowledge from the domain experts that would not emerge during a classical risk analysis.

14. SUBJECT TERMS Information Assurance, Computer Security, Decision Support	**15. NUMBER OF PAGES** 128
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

THIS PAGE INTENTIONALLY LEFT BLANK

PRIORITIZATION OF INFORMATION ASSURANCE (IA) TECHNOLOGY IN A RESOURCE CONSTRAINED ENVIRONMENT

Carl Phillip Brodhun III
Major, United States Marine Corps
B.A., Norwich University, 1990

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
December 2001

Author: ______________________________
Carl Phillip Brodhun III

Approved by: Cynthia E. Irvine
____
Cynthia E. Irvine, Thesis Advisor

____
Raymond R. Buettner, Thesis Advisor

William J Haga
____
William J. Haga, Associate Thesis Advisor

Dan C Boger
____
for George Conner, Chairman, Information Sciences Department

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Classical risk analysis is a static process that does not account for rapid evolutionary or generational changes in technology and technological solutions. This thesis defines a process that expands classical risk analysis to *increase visualization* of the secuurity environment of an information system. It provides a *comparative analysis* of system attributes and encourages *focused communications* between decision-makers and information systems technicians.

Personal interviews with domain experts from four organizations were used to construct a baseline model. Face validity of the model was determined during sessions with the domain experts. The model was calibrated to two specific scenarios using a pair of surveys to set link values and establish data for the initial nodes. A verification phase compared rough results from the model with expert opinion.

The model *evaluated, prioritized and graphically illustrated* shortfalls within two information systems based on the relative importance of specific criteria established by the domain experts. And, it facilitated the extraction of implicit or tacit knowledge from the domain experts that would not emerge during a classical risk analysis.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The thesis has given me a reason to go to class for twenty-one of twenty-eight months, but the best part of my education at the Naval Postgraduate School has been the opportunity to meet and work with all of the people who have helped nurture, cajole, encourage, and drag my dim concept of more effectively prioritizing IA expenditures into the light of day.

I would like to thank the personnel of C4, Headquarters Marine Corps, specifically: Mrs. Debra Filippi, Deputy Director, C4 (CIO); Colonel Robert Baker, Chief, Plans and Policies, C4; and Ms. Elaine Cassara, Branch Head, Information Assurance, C4.

Special thanks must go out to the personnel of the Marine Corps Information Technology and Network Operations Center and the Joint Information Operations Center for their participation in the modeling process. Without their forbearance and help, this application would have remained in academic limbo.

The supporting cast includes Dr. Julie Rosen and Wayne Smith, creators of SIAM and excellent technical critics for my new application of their software; the NMCI IA team from SPAWAR-SD; key IA players at the NSA; and many others. My deepest thanks to both groups and all of the others from DoN CIO, IATFF, NPS, and the commercial sector whose expressed interest in the possibilities of a new tool kept me motivated over the months.

Obviously the support and motivation received from my advisors has been crucial. Professor Cynthia Irvine's knowledge in the field dogged determination to keep me on track…Professor Bill Haga's quiet guidance and steadfast refusal to allow me to 'wax esoteric'…and LCDR Ray Buettner's strong belief in the validity of the project, his friendship, and resource support. Without the three of them, this thesis would be much less than it has become.

Close friends have also served as excellent sounding boards (willing or unwilling). Captain Ann Summers, USA; Captain Holly Korzilius, USMC; Ms. Alexis Waddel, and MSgt Bob Massie, USMC (ret.) have led the way. I really appreciate your willingness to listen patiently as I prattled on.

Thanks go to my family for providing me with my motivation to succeed. And, my deepest appreciation goes to Ms. Jennifer Dianto. Her dedication to her own work has kept me focused on mine; her professionalism has kept me on track in the final hours; and her deep friendship has made me realize why the long hours and sweat were all worthwhile. Thank you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. RISK ANALYSIS ILLUSTRATED

Incomplete risk analyses often leaves vulnerabilities in information resource management systems and opens organizations up to expensive recoveries after those vulnerabilities have been exploited. Organizational resource allocations are frequently based on the most recently touted hack, crack, or chink in the 'defense-in-depth' armor.

Classical risk assessment is time consuming and completely static. It does not provide a collaborative environment that dynamically supports enhanced communications between technicians and decision-makers. "What-if" forecasting in support of changing situations or requirements is not easily conducted using either quantitative or classical qualitative techniques.

Risk analysis is a process undertaken to determine the exposures within a system and their potential harm. The process forces the systematic study of the exposures and assists in justifying the type or quantity of security required. [Pfleeger, 1997] Although, the purpose of the model is to support the justification of security processes or techniques, just as classical risk analysis does. This model does not conduct risk assessments in the classical sense. Rather, it expands on classical methods in order to:

- Enhance visualization of the target system;
- Provide a dynamic evaluation environment, responsive to rapidly changing information assurance requirements;
- And, encourage dialog between decision-makers and technicians through the provision of a common frame of reference.

The model evaluates, prioritizes, and graphically illustrates shortfalls within the modeled system based on the relative importance of specific criteria as established by domain experts. It also facilitates the extraction of implicit or tacit knowledge from these same domain experts that would not emerge during classical risk analysis.

B. BACKGROUND

Intellectually, decision-makers understand the importance of information assurance across the enterprise. However, the resource holders do not really understand the depth of the issues, additionally, security costs money. It is difficult to justify IA expenditures for existing systems, when there is no visible threat, let alone allocate resources on IA requirements for systems still in the vapor-ware stages. The result is that decision-makers are pulled into the vicious cycle of throwing money at a problem after the problem has already occurred. We implement, assess, and patch…instead of designing integrated systems and families of systems with IA considered from the beginning.

Technicians suffer from an opposing set of problems. Although intimately familiar with the challenges of operating in the IA world, they are frequently hamstrung by their own specialization and consistently suffer from a dearth of resources. The system almost encourages this in that highly skilled specialists are prized…they are selected, trained and rewarded based on the depth of their knowledge, not the breadth. The people that see information systems from a big picture stand point do not see systems until AFTER they have been developed. At that point, it is often "…back to the drawing board…", instituting long delays and significant cost increases.

A long-run view during the requirements definition phase is critical. Nevertheless, this can have its drawbacks as well. Decision-makers that take long-term views run the risk of becoming locked into strategies designed to solve yesterday's crisis. In many cases, this can prove to be as detrimental, if not more so, than the expenses associated with treating all problems as "one-time" events.

C. BENEFITS OF THIS THESIS

The work encompassed in this thesis is a first step in bridging the gap between decision-makers and technicians. It provides a process that can be used to evaluate extant firewall systems or assist in the strategic allocation of resources towards information assurance. The model developed during this research increases visualization of the environment being modeled; it provides a dynamic environment for comparative analysis of system attributes; and, it encourages more focused communications between decision-makers and technicians. This combination of characteristics makes it unique.

Without expansion upon classical risk analysis techniques, organizations will continue to invest in emergency situations without thought for incremental benefits. Solid planning and incremental investment, using a tool such as that presented her e, can mitigate the risks of throwing good money after bad. Incremental investments in information assurance have the potential to offer exponential increases in security posture. This thesis offers a process by which those incremental investments can be prioritized in relation to organizational security goals.

II. LITERATURE REVIEW

This chapter will provide the backdrop for further discussion of the central model. The text will introduce some principles of information security and information assurance; define a framework for managing secure systems; and detail an overview of the Situational Influence Assessment Module (SIAM).

A. INTRODUCTION TO COMPUTER SECURITY AND INFORMATION ASSURANCE

The National Security Telecommunications and Information Systems Security Instruction, No. 4009, defines computer security as "…measures and controls that ensure confidentiality, integrity, and availability of information systems[IS] assets including hardware, software, firmware, and information being processed, stored, and communicated." [NSTISSI 4009, 1999]

Organizations often field software and/or disparate hardware, assess its performance and problems, then create or apply patches to fix the discovered bugs and loopholes. This process leaves much to be desired in that it does not allow for the coherent integration of the system at large. Murray states: "We will not achieve effective, much less efficient, security without an enterprise-wide design and a coherent management system." [in Krause & Tipton, 1999a] While a coherent, integrated approach is a natural process in enterprise network design, system security is often left as an after-thought.

Ranum [1996] asked "What is 'secure'?" It appears to be a simple question, but is it really? He went on to propose that "'secure' by itself doesn't mean anything."

Is secure a meaningful term in the abstract? The word secure, as it relates to information assurance and computer security, is often defined by the result of a technological implementation process. Ergo: suppose that an organization installed a firewall (or access controls, or physical security, etc.). One might suppose that the organization is 'digitally secure'. It is possible that this measure contributes to overall security; however, without an understanding of how the installation of a firewall contributes to the enforcement of enterprise security policy, it is ad hoc. Being secure is the result of an iterative, rigorous, development of an information assurance policy and requirements determination. Without it, security is nothing more than smoke and mirrors until requirements are generated in support of an information assurance [IA] strategy.

Four basic questions must be asked in order to generate a set of security requirements:

- What is at risk?
- How hard is an adversary willing to work for unauthorized access or system modification?
- What is the loss involved if someone succeeds in gaining unauthorized access? How much damage can be done?
- How much is an organization willing to pay to defend or recover its assets? (This in terms of how much it will cost in time, money and lost productivity.)

Although certainly not an exhaustive list, the satisfaction of the requirements generated by these questions enables one to begin establishing a reasonable system that balances accessibility for authorized users with security from ne'er-do-wells. Unfortunately, the answers to these questions are often along the lines of: 'everything'; 'very hard'; 'a lot'; and 'as little as they can get away with'. To paraphrase the industry, security is an inevitable series of tradeoffs: security vs. accessibility; functionality vs. ease of use; everything vs. costs. This thesis will attempt to clarify some of the impacts that these tradeoffs may have upon the overall status of a system as system security requirements are satisfied. "The goal," writes Denning [1999a], "is not to deny access – which in itself is a method of attack – but rather to deny only unauthorized access and to do so as economically and inconspicuously as possible."

1. Information Security

The Joint Chiefs of Staff defines information security as "…the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional." [JCS, 2001]

2. Information Assurance (IA)

DOD has defined Information Assurance as "Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." [DoDD 5160.54]

3. Information Systems Security (INFOSEC)

According to the National Security Telecommunications and Information Systems Security Committee, information systems security is "…the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users or the provision of service to unauthorized users (including those measures necessary to detect, document, and counter such threats)." [NSTISSI 4009, 1999]

B. FRAMEWORK FOR MANAGING SECURE SYSTEMS

In many ways the ability to create a secure, digital nirvana is something of an art form. It involves the focus of a specialist capable of leveraging significant experience, one with an in-depth knowledge of technology and potential threats, and someone capable of interpreting strategic organizational goals into well-defined security requirements. In order to begin framing the challenges involved in the development and implementation of a robust, integrated information security solution, a security framework must first be defined. This framework is essential to understanding the critical interactions between policy, planning, and architecture. For our purposes, this framework will be composed of three distinct parts:

1. The enterprise security policy.
2. The organizational security policy.
3. Automated security policies.

There has been, and continues to be, some debate over what the definition of a "security policy" really is. Sterne [1991] argues several points:

- That the definition of the term "security policy" is fundamental to computer security concepts and terminology.
- That the lack of a coherent definition acts as an obstacle to routine discourse on the subject of computer security.
- That a clear, concise definition of "security policy" is essential for resolving key issues within and establishing the scope of research, systems engineering and standardization efforts.

First, an enterprise cannot develop solid, coherent security architecture that effectively supports organizational goals without those goals having been defined in some policy statement. If no one understands what security policy is comprised of there is no effective way to communicate strategic organizational security goals. This leads directly into Sterne's second assertion, i.e. how does one have intelligent, meaningful conversation on information assurance and computer security for systems supporting an organization if there is no baseline definition of what policy is? In the end, clearly defined organizational goals allow people to address concerns and issues in terms of specific solutions.

For the purpose of this thesis, the following definitions will apply:

1. Enterprise Security Policy

The enterprise security policy is the foundation document, or collection of documents, in the information security framework. At its highest level, this policy will define enterprise goals and strategy as they relate to information assurance. However, subordinate elements may have similar framework foundations built on a smaller scale.

This document represents a strategic view of information assurance and security within the enterprise or organization. In general, it should state big-picture beliefs, goals, and objectives of the organization as well as the general means that will be used to attain them. As with commanders' intent and mission-based orders in the military, an enterprise security policy provides guidance and direction to subordinate elements concerning ***what*** should be done without discussing technical implementations.

The enterprise security policy contains key elements that define the long-range goals of the organization. Sterne [1991] defines these goals, called Security Policy Objectives, as "…statement[s] of intent to protect an identified resource from unauthorized use." A stipulation of this definition is that an objective is "…meaningful to an organization only if the organization owns or controls the resource to be protected."

Understanding the limits of one's influence in the network-centric world, and therefore the boundaries of one's enclave is crucial. Establishing a measure of 'reasonable internal and external security' is essential. However, If an organization does not own a specific asset, service, or communications node required to support communications there are only two choices that can be made: either refuse to connect to the external world; or establish a trust relationship with those who do own the asset, service or node in question. These trust relationships comprise an ever-expanding web that exceeds the scope of this thesis.

2. Organizational Security Policy

Sterne [1991] specifies the organizational security policy as: "…the set of laws, rules, and practices that regulate how an organization manages, protects, and distributes resources to achieve specified security policy objectives." In other words, the organizational security policy is an abstract; a statement of what the enterprise intends to do. The organizational security policy should frame how the goals and objectives put forth in the enterprise policy will manifest themselves in the automated security policies.

3. Automated Security Policy

This refers to an actual implementation policy on a given piece of hardware or in a software application. These are the methods used by software and devices to execute information assurance through out the system. These technical policies are central to the creation of an architectural framework, implemented automatically by hardware or software, and govern the day-to-day operations of the assembled systems. Sterne [1991] defines these types of policy as "…the set of restrictions and properties that specify how a computing system prevents information and computing resources from being used to violate an *organizational security policy*." Modern examples of these policies might be automatically executed intrusion detection and logging, automated controls within boundary layer security devices, or identification and authorization routines enacted by an operating system during network log-ins.

C. THE SITUATIONAL INFLUENCE ASSESSMENT MODULE (SIAM)

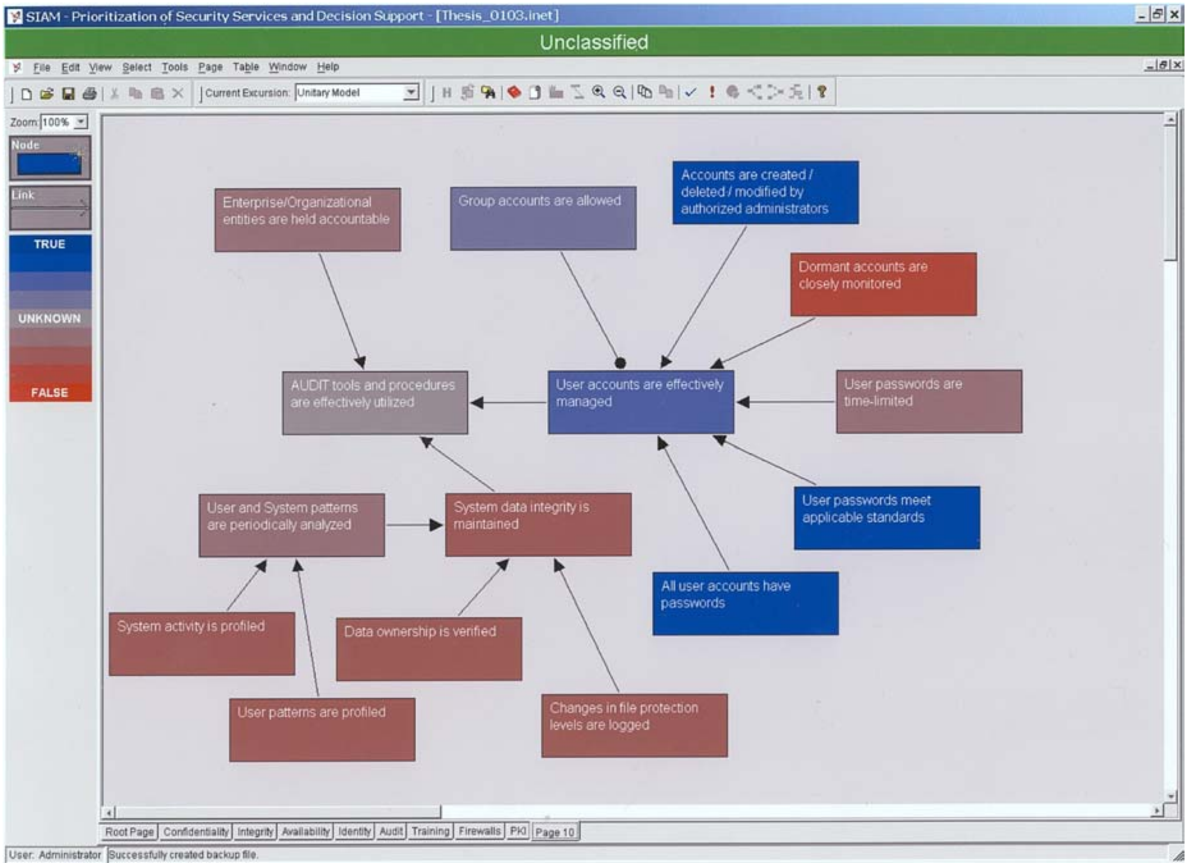
Created in the early nineties by Rosen and Smith [1994] of Science Applications International Corporation, SIAM is a software application that enhances the visualization of influences exercised by dissimilar attributes upon a central premise through the use of "influence net" technology. The use of the influence net modeling technique significantly improves the capability of the modeler to portray complex inter-relationships in an imperfect and uncertain world. SIAM simplifies the modeling process through the use of an intuitive graphical interface, robust analysis tools, and extensive documentation capabilities.

Complex problems are often solved in group environments where the experience of multiple subject matter experts may be leveraged. Two sets of techniques frequently used are: "Seminars, workshops, and informal communications that are aimed at extracting subjective, but valid, knowledge from subject matter experts; and mathematical and computer-based models/simulations that attempt to estimate current and future states of "physics based" phenomena." [Rosen and Smith, 1996] In both cases, the underlying reasoning and documentation that supported a specific course of action is often lost.

SIAM offers a structured approach to these discussions that supports real-time collaboration among subject-matter experts and, if the process is properly executed, retains the source material, justifications, and reasoning that directly impacts a decision set. "The success of this structured approach lies in the early identification of events and interrelationships that have great potential to influence the ultimate outcome of a situation." [Rosen and Smith, 1999]

1. Influence Nets

Influence nodes and links comprise the topology of an influence net that may be used to facilitate communications between a group of 'experts' and a decision-maker or set of decision-makers. Nodes are color coded from red (inhibiting) to blue (promoting) in order to visually orient users to value identification.



SIAM - Prioritization of Security Services and Decision Support - [Thesis_0103.inet]

Current Excursion: Unitary Model

Zoom: 100%

User: Administrator

Successfully created backup file.

Unclassified
File
Edit
View
Select
Tools
Page
Table
Window
Help
Node
Link
TRUE
UNKNOWN
FALSE
Enterprise/Organizational entities are held accountable
Group accounts are allowed
Accounts are created / deleted / modified by authorized administrators
Dormant accounts are closely monitored
AUDIT tools and procedures are effectively utilized
User accounts are effectively managed
User passwords are time-limited
User passwords meet applicable standards
User and System patterns are periodically analyzed
System data integrity is maintained
All user accounts have passwords
System activity is profiled
Data ownership is verified
User patterns are profiled
Changes in file protection levels are logged
Root Page
Confidentiality
Integrity
Availability
Identity
Audit
Training
Firewalls
PKI
Page 10

Figure 1: Sample Influence Net Diagram

The model's nodes depict events that are incorporated into cause and effect relationships within a situation or decision process under consideration. The influence links between the nodes (representing causes and effects) graphically illustrate the causal relationship between a pair of connected events. Within SIAM, this relationship may be either "reinforcing" (event A increases the likelihood of event B) or reversing (the occurrence of A reduces the likelihood of B). Arrowhead terminators identify reinforcing links, and solid circle terminators identify reversing links. [Figure 1]

Decision-makers often require the capability to examine multiple courses of action in real or near-real time. These decisions may range from those concerning short-fused procurements to those with the potential to mitigate the effects of an impending crisis. "In order to provide a real-time analytical capability for situations fraught with uncertainty, a rigorous mathematical foundation, such as Bayesian inference networks, is required." [Rosen and Smith, 1999] The problem with using traditional (mathematically-based) processes is that the highly structured, observable, repeatable measurements required often do not exist or are not available in support of a subjective decision-making process. Rosen and Smith [1999], in conjunction with members of George Mason University's C3I Center for Excellence, developed the Causal Strengths (CAST) algorithm. This evolutionary approach to model construction "…allows users to assign expert judgments to the likelihood of initial-state events and the strengths of the influencing relationship between cause and effect. These parameters are then employed in the standard forward belief propagation to compute the cumulative impact of all causes (direct and indirect) on each event in the model's topology." [Rosen and Smith, 1999] The CAST algorithm is the heart of the SIAM modeling engine.

2. SIAM Explained

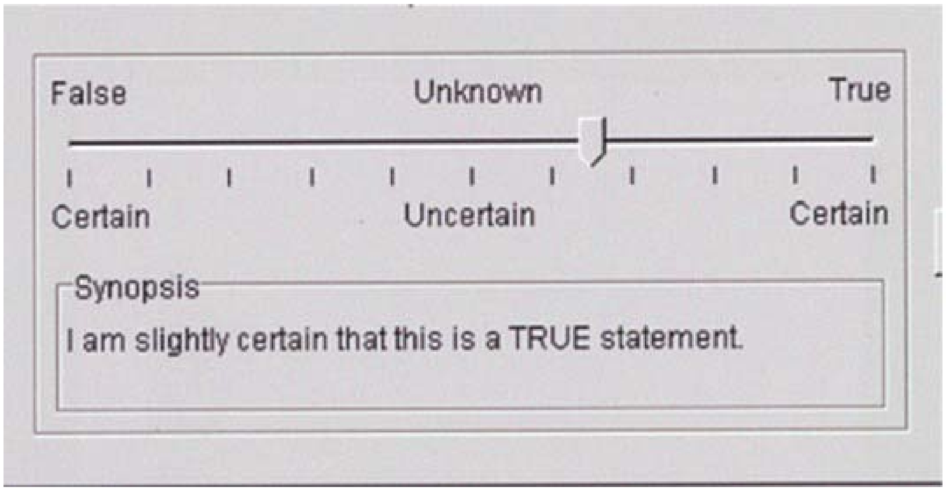
SIAM is a software application that provides a graphical interface and underlying algorithmic engine combining two well established methods of decision analysis: the mathematical community's Bayesian inference net analysis; and influence diagramming techniques used within operations research. Once an influence net, as described above, has been created, planners and decision-makers must formulate the answers to several questions:

- Which of several selected causes has the greatest impact on the identified effect?
- Of all the factors included in the model, which one (or two or three) has the greatest potential to change the situation, assuming other factors remain the same?
- What is the chance that a factor will occur changes as the situation evolves? How is the desired outcome affected?
- If I apply an influence to one or more factors, what are the unintended side effects?

[Rosen and Smith, 1999]

Experts can often address these questions within their own domain of expertise; however, when confronted with problems that cut across the breadth of enterprise issues or potentially impact significantly different stakeholders, the analytical ability of individuals rapidly comes up short. SIAM facilitates the construction and analysis of Influence Net models.

Initial nodes are those nodes around the external edge of the net—events that have no explicitly modeled cause. Values assigned to these nodes represent the initial state of the environment or issue(s) being modeled. The current belief of these nodes is manually assigned by the modeler based upon input from an expert or group of experts. The belief slider bar, found on the node properties page, is used to adjust the current belief value of the node. The value of this current belief is then used, in conjunction with the nodal link values of the model, to calculate a value for all descendent nodes, including the model's root node. Values on the belief slider bar range from 'very certain the event is false' on the left side through the 'I don't have a clue' stage in the center to 'utter certainty that the event is true' on the far right. [Figure 2]



I am slightly certain that this is a TRUE statement.

Figure 2: The SIAM Belief Slider

Current certification and accreditation procedures evaluate systems at a given moment in time. Rather than blindly taking a snapshot at a single point in time, the SIAM environment assists in "…modeling the situation to understand what the potential pressure points for change might be." [Rosen and Smith, 1999] SIAM offers an environment in which the modeler can dynamically manipulate the model in order to conduct real-time analysis.

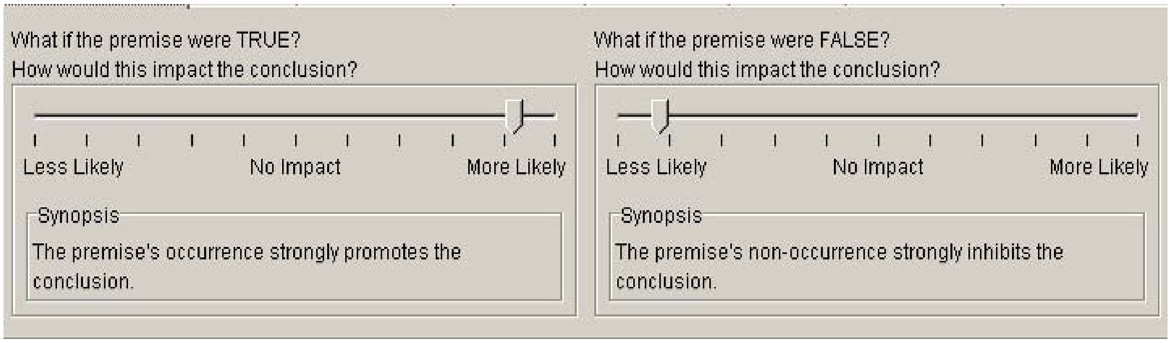
The ability to set the link strengths of the causal parameters is critical when modeling these potential pressure points. SIAM requires the modeler to answer two opposing causal strength parameters:

- "In a future where the influencing factor ***were true***, would the effect be more or less likely to occur?

- On the other hand, in an alternate future where the influencing factor ***were false***, would the effect be more or less likely to occur?"

[Rosen and Smith, 1999]

As stated previously, the links may be either reinforcing, the strength of the link supports the positive influence of the node; or reversing, where the positive nodal value has a negative influence on the resulting effect. The mechanics of setting the link strength values is similar to using the belief slider. [Figure 3]



What if the premise were TRUE?
How would this impact the conclusion?

The premise's occurrence strongly promotes the conclusion.

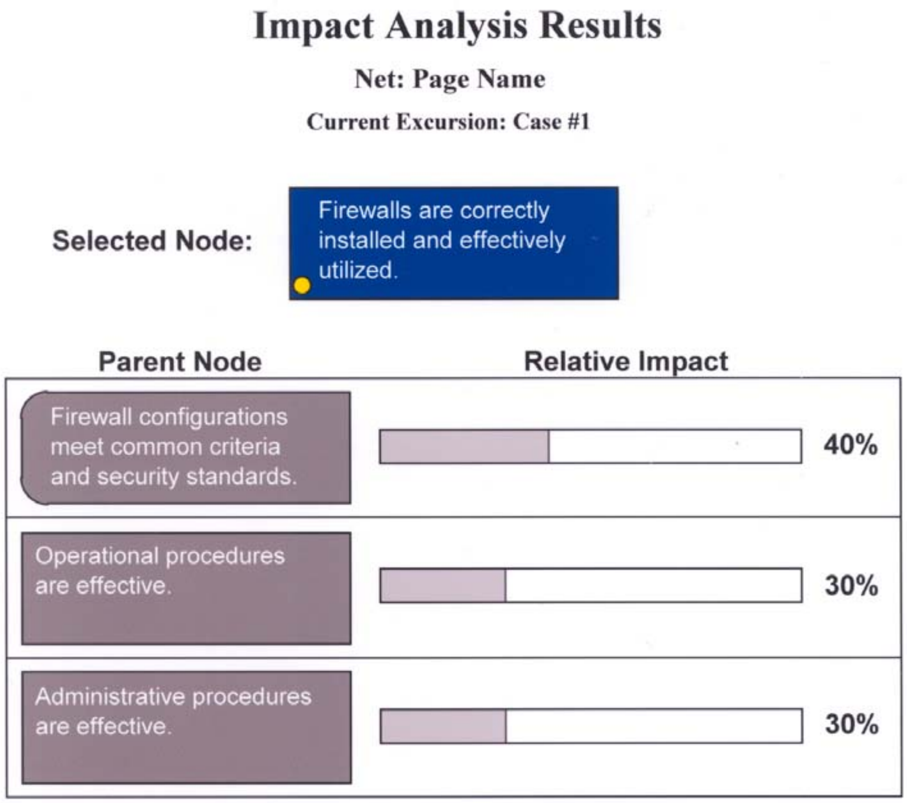
What if the premise were FALSE?
How would this impact the conclusion?

The premise's non-occurrence strongly inhibits the conclusion.

Figure 3: The SIAM Link Value Slider Bars

3. Applying SIAM

The operational benefits of SIAM often are realized well after the models are constructed. However, the learning process that occurs during model construction is critical. The development of a model, that accurately reflects the modeled environment, forces technicians and decision-makers to form more accurate and increasingly detailed assessments of their surroundings. This requirements determination process often identifies problems or issues that had been previously obscured under layers of technology or procedure. From an operational and managerial point of view, the tools and techniques available for the analysis of a given model are robust and easy to use. Alternate futures are simple to explore. Belief values for a given node or nodes can be changed and the display refreshed using the "Belief Evaluation" button. By adjusting link strengths on-the-fly, modelers can compensate for an incorrect intuitive supposition that a particular factor holds little importance. The automated belief evaluation algorithm can display overlooked or forgotten paths of influence. Results generated can indicate whether several paths of relatively weak influence combine to produce an unexpected strongly influenced outcome. There are two major techniques available for the analysis of SIAM models: impact analysis and sensitivity analysis. The impact analysis “allows users to identify whether or not a single ‘silver bullet’ exists.” [Rosen and Smith, 1999] If no single factor surfaces with an overwhelming influence, a subset of influence factors must then be used to provide a reasonably sufficient impact on the decision process. Figure 4 shows the relative impacts of factors on the selected outcome shown at the top of the graph. Although simplistic, the figure demonstrates how a factor may have an overwhelming impact on a given result.



Impact Analysis Results

Net: Page Name

Current Excursion: Case #1

Selected Node: Firewalls are correctly installed and effectively utilized.

Parent Node	Relative Impact
Firewall configurations meet common criteria and security standards.	40%
Operational procedures are effective.	30%
Administrative procedures are effective.	30%

Figure 4: SIAM Impact Analysis Results

The sensitivity analysis tool allows slightly finer control in identifying factors that can be used to significantly influence a given outcome. The results of this analysis identifies factors that have a greater or lesser potential to alter the outcome of a selected event. [Figure 5] Factors with wider shaded regions on the right hand side of the display have a potentially greater effect on the selected outcome. As shown in the figure, sensitivity can be high or low, based on the value and direction of the nodal relationships. Several parameters, including the degree of multi-path connectivity between influencing factors and influenced outcomes, and the strengths of each pair-wise cause-effect link exercise control over the factor sensitivity.

Pressure point sensitivity analysis also provides a graphical representation of the degree to which an outcome may be affected by an event. In Figure 5, the opportunity for the events to promote the outcome is about equal. However, the lack of knowledge concerning operating system [OS] feature sets has the potential to significantly inhibit the outcome that an OS is mature and stable.

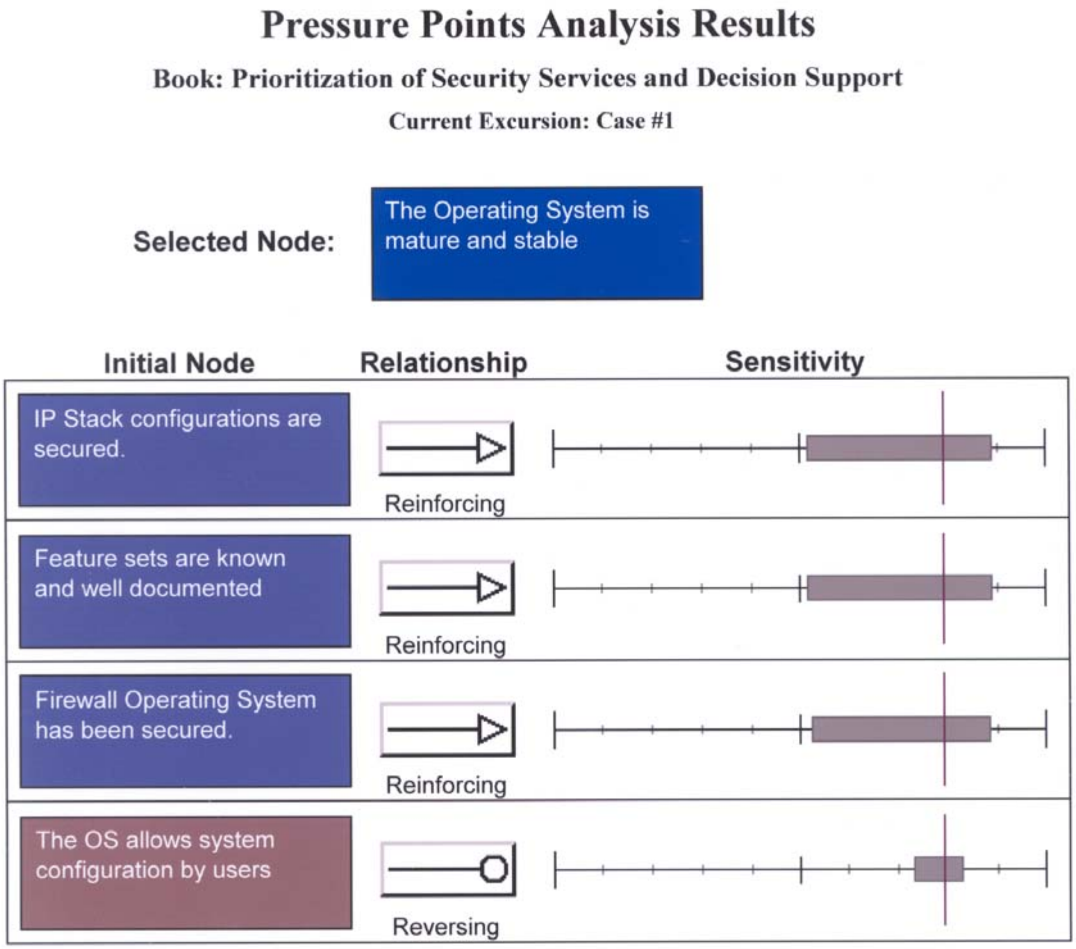


Figure 5: SIAM Pressure Point Analysis Results

Other sensitivity analysis tools within SIAM allow modelers to analyze and compare the:

- Sensitivity of a desired effect to combinations of influencing factors;

- Sensitivity of a desired effect to selected factors as influencing relationships change over time; and
- Sensitivity of a desired effect to selected factors as alternate future scenarios, called excursions, are triggered.

[Rosen and Smith, 1999]

In this thesis, SIAM will be used to construct an influence net illustrating the factors and events surrounding a specific firewall implementation. The analysis tools will enable an accurate portrayal of how factors influence selected critical outcomes and how pressure point sensitivity in the model may be manipulated to increase the effectiveness of actions taken in management of the modeled environment. Using these tools, the comparison of a specific firewall implementation to a written policy and set of "best practices" can be made effectively.

III. THE MODEL: ITS DEVELOPMENT AND APPLICATION

Previous chapters provide an overview of information assurance and the technical details of SIAM. This chapter provides:

- A short description of the model characteristics.
- The process used to create it.
- An overview of the data collection and validation processes.
- And, a quick précis on the analysis strategy.

A. CONCEPT AND CONTEXT

The original concept was that a model of the enterprise security policy could be constructed that would assist in determining where an organization's information assurance resources should be most effectively allocated. In pursuit of this goal, it was necessary to understand the formulation of strategic policy and system planning for information assurance. Research spanned numerous publications, articles, and personal interviews. Input from agencies such as the National Security Agency, Space and Naval Warfare Systems Center, San Diego [PMW-161], and the Marine Corps Information Technology & Network Operations Center has been critical.

Confidentiality, integrity, and availability are key objectives in information assurance. [Pfleeger, 1997; Stallings, 2000; Sterne, 1991] However, further research revealed that identification (authentication and authorization), auditing, and training are critical supporting processes enabling the achievement of the three goals listed above.

None of this is new; however, identification and auditing are often relegated to steerage status and training, beyond that required for administrators to be effective, is generally ignored. Of the three supporting processes, training has received the least attention in the literature. Without proper training administrators will be incapable of maximizing the utility and performance of installed security-oriented technology. Ignorant or uninformed users represent vulnerabilities to system security. The fact that users do not "play by the rules" is often a consequence of them either, not knowing what the rules are, or not understanding why the rules are important to the well-being of the enterprise. [Kabay, 1996] People tend to focus on efficient job completion versus security measures. Kaeo [1999] supports this when she says that, "…security measures are [often seen as] more of a nuisance than a help."

Based on initial research, I developed a top level influence net built around the root node: "Required levels of Security Service have been achieved." To be an effective root node (strategic objective), the required levels of service must be well defined. The top level of the strategic model shows the six primary security functions. [Figure 1] The six categories of security service that I defined as top-level parents to the root node were:

- *Confidentiality is maintained*
- *Integrity controls are effective*
- *Availability of information meets applicable standards* (formal expectations within an organization)
- *Identity procedures are adequate*
- *Audit tools and procedures are effectively utilized*
- *Training standards have been met*

Recall from the Background [Chapter II] that parent nodes are those nodes within the model that *exert an influence* on the child (or target) node. In Figure 6, the root node is the child of all six parents.

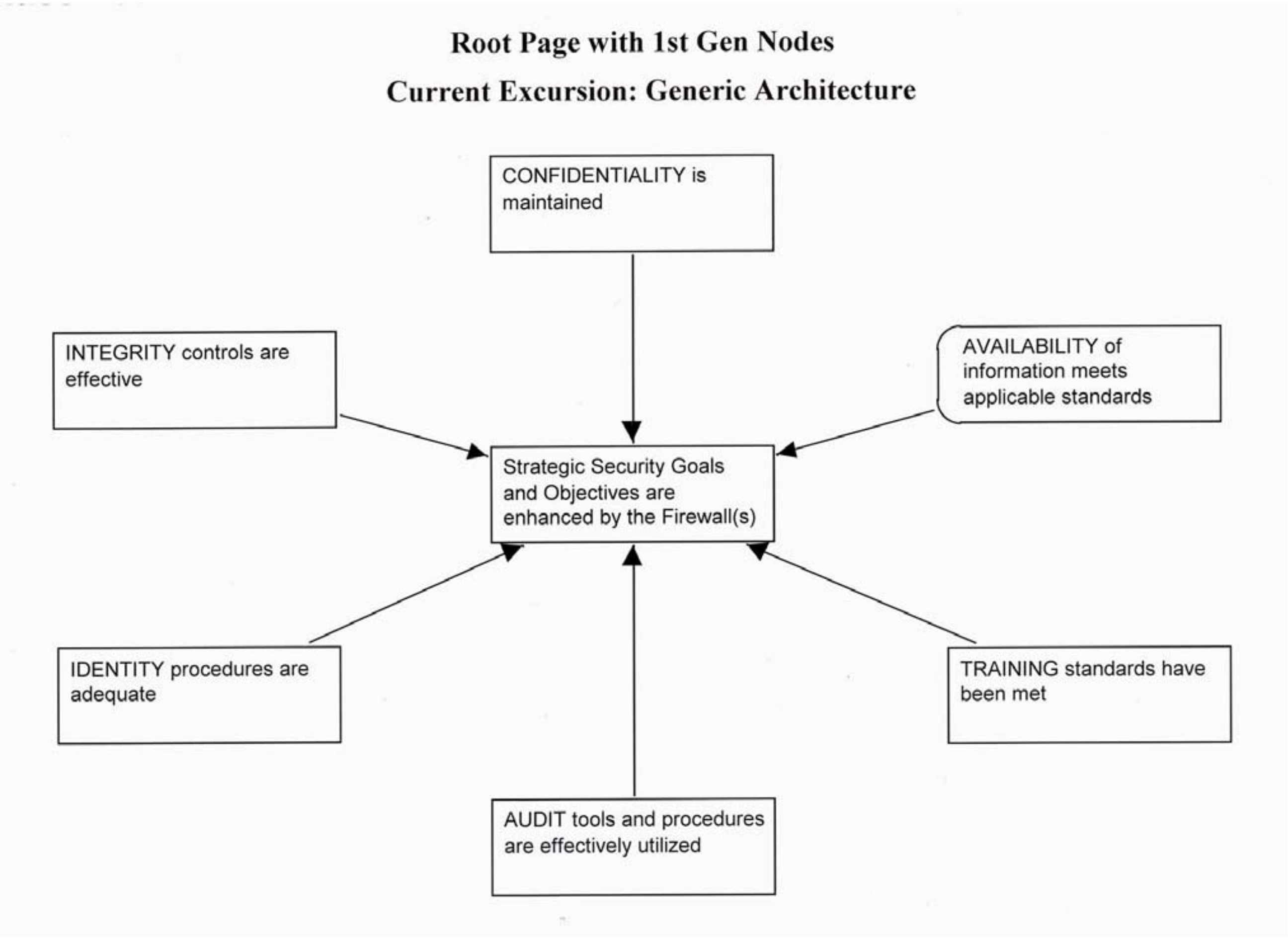

Root Page with 1st Gen Nodes
Current Excursion: Generic Architecture
CONFIDENTIALITY is maintained
INTEGRITY controls are effective
AVAILABILITY of information meets applicable standards
Strategic Security Goals and Objectives are enhanced by the Firewall(s)
IDENTITY procedures are adequate
TRAINING standards have been met
AUDIT tools and procedures are effectively utilized

Figure 6: Initial Top Level IA Net

B. THE MODEL TODAY

This thesis focuses on a specific firewall implementation as implementation influences the goals: *Integrity controls are effective*; and that, *Availability of information [within the system] meets applicable standards*. Applicability of the tool is demonstrated through the analysis and reporting mechanisms that can be applied to a practical implementation. 'Drilling down' or navigating through the model from the conceptual top level to the specific implementation level exercises this functionality.

1. Orientation

The model has been layered to better address the diversity of processes that influence effective information assurance. Within the model [Figure 7], parent nodes focusing on system availability (2) and integrity (3) support the root node (1). System availability (2) and integrity

(3) are both dependent on, among other criteria, logical security (as opposed to physical security) (4), and firewalls (5) contribute to logical security. The effectiveness offered by the firewall relies on the quality of the installation and configuration (6), as well as the effectiveness of operational (7) and administrative (8) procedures. Of course, other technical solutions such as intrusion detection, content scanning of email, etc., contribute to the logical security of a network environment. These other classes of technology are not specifically addressed in this thesis but should be considered targets for integration in the future.

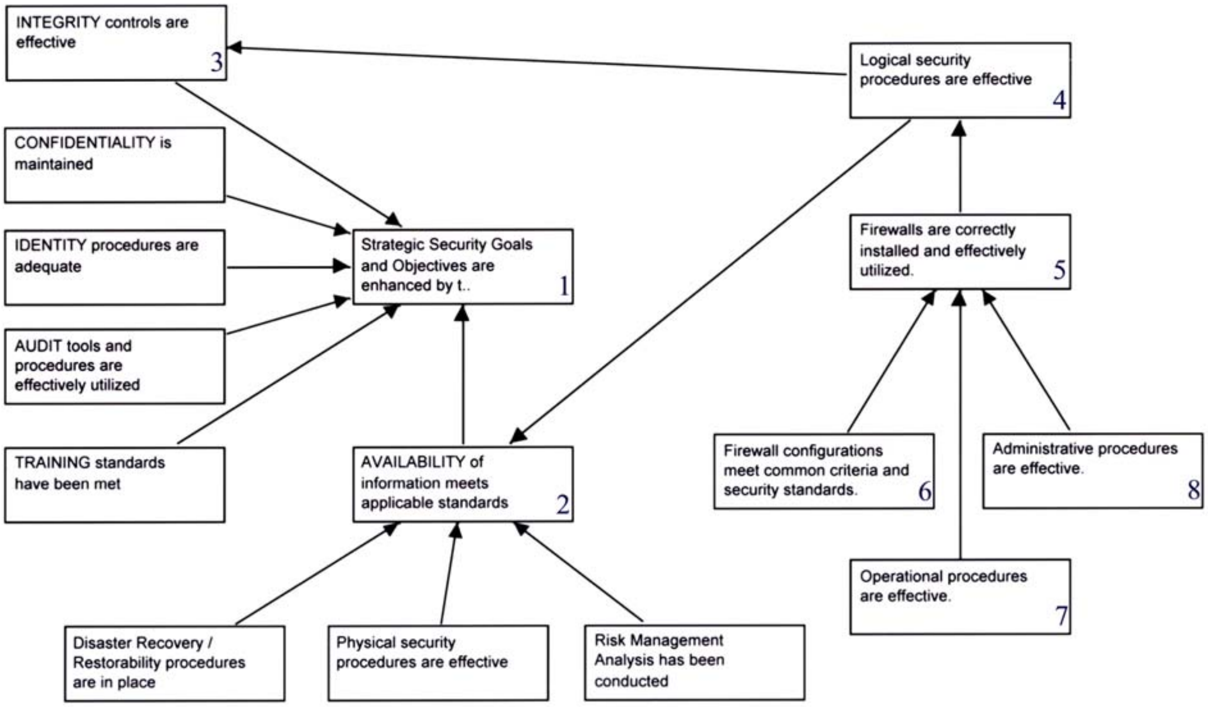

INTEGRITY controls are effective 3
Logical security procedures are effective 4
CONFIDENTIALITY is maintained
IDENTITY procedures are adequate
Strategic Security Goals and Objectives are enhanced by t.. 1
Firewalls are correctly installed and effectively utilized. 5
AUDIT tools and procedures are effectively utilized
TRAINING standards have been met
AVAILABILITY of information meets applicable standards 2
Firewall configurations meet common criteria and security standards. 6
Administrative procedures are effective. 8
Operational procedures are effective. 7
Disaster Recovery / Restorability procedures are in place
Physical security procedures are effective
Risk Management Analysis has been conducted

Figure 7: Model Topography

The model supporting this research is broken down into three logical components: Installation and Configuration, Operations, and Administration [Figure 8], all of which directly influences the primary goal that *Firewalls are correctly installed and effectively utilized*. Each of these major divisions has been further divided into a layered set of influencing events or actions. The goal of this decomposition is to reduce event possibilities to a dichotomous series of “yes” or “no” approximations.

Careful attention to model granularity is essential. SIAM is designed to calculate the relative influence of all model nodes, via the nodal values and link strengths, on the designated root node. Granularity can become so fine that the utility of the model may be adversely affected through diluted calculations. Similarly, models in which the initial nodes are not reduced to "yes," "no," or "maybe" answers suffer the same fate. [Chapter II]

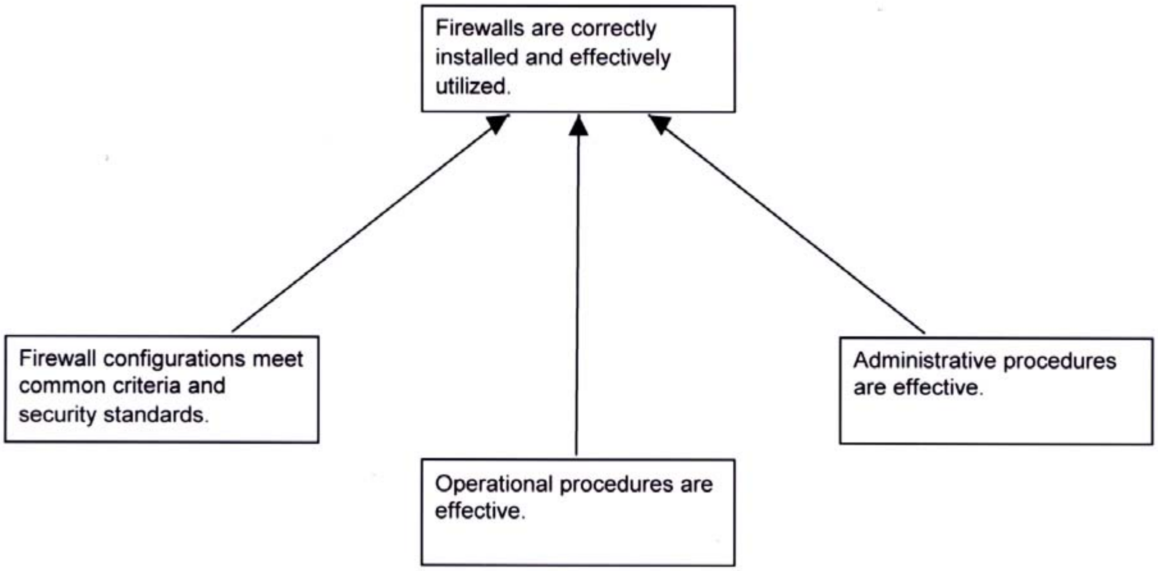

Firewalls are correctly installed and effectively utilized.
Firewall configurations meet common criteria and security standards.
Administrative procedures are effective.
Operational procedures are effective.

Figure 8: Firewall Root and Associated Parent Nodes

a. Installation and Configuration

The correct installation and configuration of a technology solution is the first step, beyond policy development and planning, toward securing a target system. Practical experience among domain experts demonstrates that securing a system is significantly easier when installation is done correctly the first time than it is to find and repair all of the possible weaknesses when the installation is not done correctly. Firewall vulnerabilities are frequently published on the Internet and in trade periodicals. This places firewall administrators on a constant 'assess and patch' cycle. A weak installation merely exacerbates this problem.

Requirements for reasonably secure firewall implementations are well documented. Commonly accepted "best practices" [NIST], the Information Technology Standards Guidance [USN ITSG, 1999], and specific organizational firewall policies or recommendations, such as those found in the Marine Corps [USMC, 2000] and Navy [USN, 1999], help to clarify firewall requirements before actual operation.

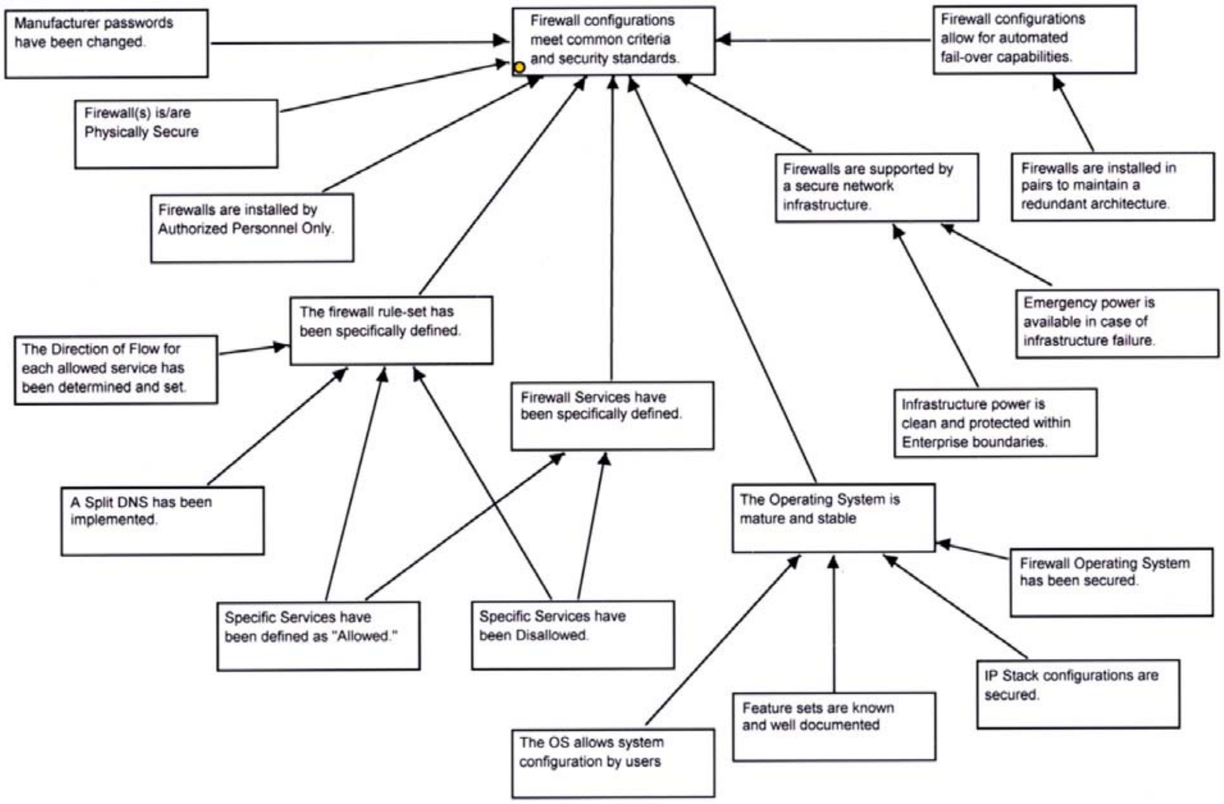

Manufacturer passwords have been changed.
Firewall configurations meet common criteria and security standards.
Firewall configurations allow for automated fail-over capabilities.
Firewall(s) is/are Physically Secure
Firewalls are installed by Authorized Personnel Only.
Firewalls are supported by a secure network infrastructure.
Firewalls are installed in pairs to maintain a redundant architecture.
The firewall rule-set has been specifically defined.
The Direction of Flow for each allowed service has been determined and set.
Emergency power is available in case of infrastructure failure.
Firewall Services have been specifically defined.
Infrastructure power is clean and protected within Enterprise boundaries.
A Split DNS has been implemented.
The Operating System is mature and stable
Firewall Operating System has been secured.
Specific Services have been defined as "Allowed."
Specific Services have been Disallowed.
IP Stack configurations are secured.
Feature sets are known and well documented
The OS allows system configuration by users

Figure 9: Installation and Configuration

Figure 9 shows the topography of the installation and configuration segment of the model. One challenge with the model is allowing for binary influence nodes. *Manufacturer passwords have been changed* is one such node. If the default configuration password is not changed, the system is significantly more vulnerable regardless of what other measures have been implemented. One recommendation that has been discussed between Dr. Julie Rosen, LCDR Ray Buettner, and the writer is the inclusion of a binary value capability within SIAM. The option to use a binary influence would enhance the effectiveness of this segment of the model. Specifically, if the stock password (one applied by the manufacturer) is not changed, all other processes are invalidated as the system has a potentially catastrophic weakness. [Figure 9]

b. Operations

The operations-oriented nodes shown in Figure 5 reflect a focus on requirements, incident recovery, and traffic flow. Generally, firewall operations are heavily automated. Basic rule sets are executed automatically. Firewall applications and tools constantly scan the traffic flow searching for anomalies. These tools cover diverse functions such as content scanning, mail filtering, and cueing/inspection of fragmented packets.

Even a labor-intensive event like disaster recovery is based on automated underpinnings. Supporting technologies such as intrusion detection; and supporting actions such as intrusion response, automated backups of firewall rule sets, and dynamic recovery/fail-over are important in preventing disastrous circumstances or in assisting technicians in the recovery process. [Tipton & Krause, 2000]

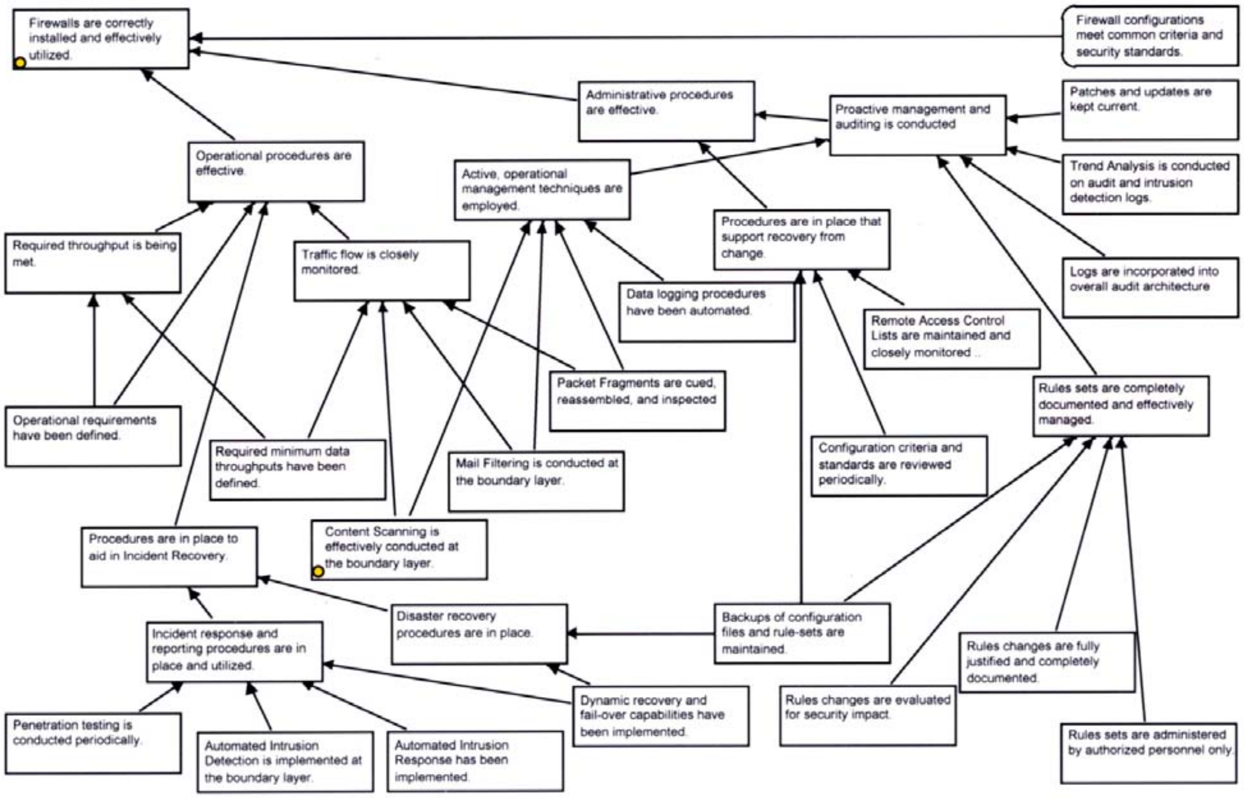

Firewalls are correctly installed and effectively utilized.
Firewall configurations meet common criteria and security standards.
Administrative procedures are effective.
Proactive management and auditing is conducted
Patches and updates are kept current.
Operational procedures are effective.
Active, operational management techniques are employed.
Trend Analysis is conducted on audit and intrusion detection logs.
Procedures are in place that support recovery from change.
Required throughput is being met.
Traffic flow is closely monitored.
Logs are incorporated into overall audit architecture
Data logging procedures have been automated.
Remote Access Control Lists are maintained and closely monitored ..
Packet Fragments are cued, reassembled, and inspected
Rules sets are completely documented and effectively managed.
Operational requirements have been defined.
Required minimum data throughputs have been defined.
Mail Filtering is conducted at the boundary layer.
Configuration criteria and standards are reviewed periodically.
Procedures are in place to aid in Incident Recovery.
Content Scanning is effectively conducted at the boundary layer.
Incident response and reporting procedures are in place and utilized.
Disaster recovery procedures are in place.
Backups of configuration files and rule-sets are maintained.
Rules changes are fully justified and completely documented.
Penetration testing is conducted periodically.
Automated Intrusion Detection is implemented at the boundary layer.
Automated Intrusion Response has been implemented.
Dynamic recovery and fail-over capabilities have been implemented.
Rules changes are evaluated for security impact.
Rules sets are administered by authorized personnel only.

Figure 10: Firewall Operations and Administration

Automated operational events have direct impacts upon the administrative management of systems. Figure 10 illustrates the connection between operational events such as content scanning or data logging and active systems management or auditing. Disaster recovery and recovery from deliberate change (those systemic changes deliberately implemented by authorized personnel as part of configuration management) are similarly connected through the automation of configuration files and rule set backups. Although often not manifest in an operational environment, these connections are intuitively correct, or have face validity, to domain experts. [MITNOC, 2001; JIOC, 2001]

c. Administration

System administration must be a proactive process, particularly in the volatile environment of firewall management. Two functions are critical:

1. Active management and auditing of system information;

2. And methods to assist in recovery from deliberate changes.

Of these two functions, interviews have indicated that secure management of changing configurations and recovering from deliberate change is often the most challenging aspect of firewall administration. [MITNOC, 2001] This is born out in the model as it shows patch application and maintenance of system backups as the two most critical items within the administrative chain. Again, the model illustrates multi-path connections [Figure 10] and influences that may not be intuitively obvious.

C. DATA COLLECTION

Data was collected to both populate the link values and set the initial node values for the model implementation tests (excursions). This data collection supported the validation of the model and face validity of the subsequent analysis results.

1. Asking the "Right Questions Right"

The questions asked, how they are framed, and how surveys are constructed all influence the quality of data collected.

At a SIAM workshop [Buettner, 2001], the various methods used to set the link and node values were discussed. One problem, raised repeatedly, was how easily results can be skewed through inattention to the formulation of questions asked to flesh out the model. This illustrates how subjective changes to the model can affect the representation of configuration processes and management of security related components.

When questioned, one group of SIAM modelers indicated that the relative influence of each parent node on each child node was set using a variation of correlation analysis techniques. These influences were rated against all of the other influences affecting the child node in question. *Ergo*, the reinforcing or reversing influence of each parent was prioritized relative to all other influences affecting the designated child node.

When this technique was used, the models suffered from influences that did not consistently represent the system environment. The influences observed were often skewed in either a reinforcing or reversing manner. The right questions may have been asked, but the focus on prioritizing the answers produced consistently invalid results.

2. Questions and Answers

Two methods are commonly used to establish link and node values for SIAM models: face-to-face encounters (interviews or collaborative conferences) and surveys/questionnaires. I have found that interviews, conducted in combination with focused surveys, have been critical to the modeling effort undertaken during this research. The surveys [Appendix C] assist in quantifying specific criteria within the model relative to the application's zero-to-one scale of values. [Chapter II] Face-to-face exposure to domain experts improves the ability of the modeler to ascertain the existence and relative importance of intangible characteristics. E.g., in most systems, the impact of user and administrator training is difficult to quantify when just using numerical systems. However, the relative influence of training on the overall security posture can be captured by a group of domain area experts.

a. Interviews

Face-to-face sessions with domain experts were conducted at the Marine Corps Information Technology/Network Operations Center, the Joint Information Operations Center, PMW-161 at the Space and Naval Warfare Command – San Diego, and the National Security Agency. These interviews were critical to establishing the face validity of the baseline model topography. The domain area experts interviewed were able to rapidly understand the model output and envision its application to real-world scenarios.

b. Surveys

Two surveys, described in Appendix C, were created to support this research effort. The first survey was designed to support the assignment of link values and the second assigned values to the model's initial nodes. Chapter 2 provides more information on both links and nodes. The surveys focus the thoughts of domain experts on the model topics and serve as a record of how the model was calibrated and results generated.

3. Setting the Values for Links and Nodes

Setting values for the links and initial modes within the model is essential (the mechanics of setting these values are covered in detail in Chapter 2.) Without detailed input from domain area experts, the model is reduced to an academic exercise conducted in a vacuum.

In order to generate consistently reliable results, the link values must be set individually (*i.e.* focus on a single parent relative to a single child), and the links must address the reinforcing or reversing nature of the influence when the parent has a logical truth value. Anecdotal evidence indicates that correlation analysis, and other techniques comparing relative link values to each other, provides dramatically skewed results. [Buettner, 2001]

D. MODEL CONSTRUCTION AND VALIDATION

Two excursions (model versions, representing the test cases, where values were added to the baseline topography) were created as a result of the test runs of the model. The first run was conducted with systems engineers from the MITNOC, and the second with the Vulnerability Assessment Team at the Joint Information Operations Center. This section details the mechanics of how the model was constructed, validated, calibrated, and verified.

1. Initial Construction

Reading applicable reference material, often out-dated before publication, is essential to understanding basic IA requirements. However, actively including domain experts, intimately involved with target systems, enables the modeler to accurately reflect the environment being modeled. The process used to construct the model for this thesis was similar to that used to build influence models in the Information Warfare domain. [Rosen and Smith, 1996] A combination of hard-copy intelligence (in this case, literature from recognized experts), and input from subject matter experts was used to develop the baseline topography of the model. [Buettner, 2001]

A range of domain experts was consulted during the initial research phase of this thesis. This process continued through the model formulation and execution phases. The input of domain experts was critical to crossing the gap between the managerial perspective and the technical implementation. Without this input the model would remain an academic, theoretical exercise.

2. Validation

Effective information security, security that efficiently secures resources and has minimal impact on the daily duties of users, is difficult. The efforts required to balance the necessity for defense in depth, intrusion detection and response, and traffic control at the firewall with accessibility and ease of use for users are massive. As such, it is very easy for a modeler to game the model to produce the desired response, instead of an accurate response based on well developed inputs. The model would then cease to accurately reflect reality. Therefore, it must be validated.

Face validity represents a reasonable simplification of reality; an “intuitive correctness” of the model to domain area experts. [Carley, 2001] The validation process, represented by establishing face validity with domain experts, is essential to continued progress with the model. The basic framework of the model should intuitively reflect the modeled environment. If the baseline topography of the model does not accurately reflect the environment being modeled then analysis results will be similarly skewed. By validating the baseline with domain experts, an ‘applicably general model with useful specificity’ is created. This validated baseline is then easily calibrated for each excursion implementation.

The focus of the validation phase is confirmation of whether the strategic goal, and web of events affecting achievement or failure in pursuit of that goal, accurately depicts the modeled environment with a reasonable degree of accuracy. A couple of questions are addressed to domain experts:

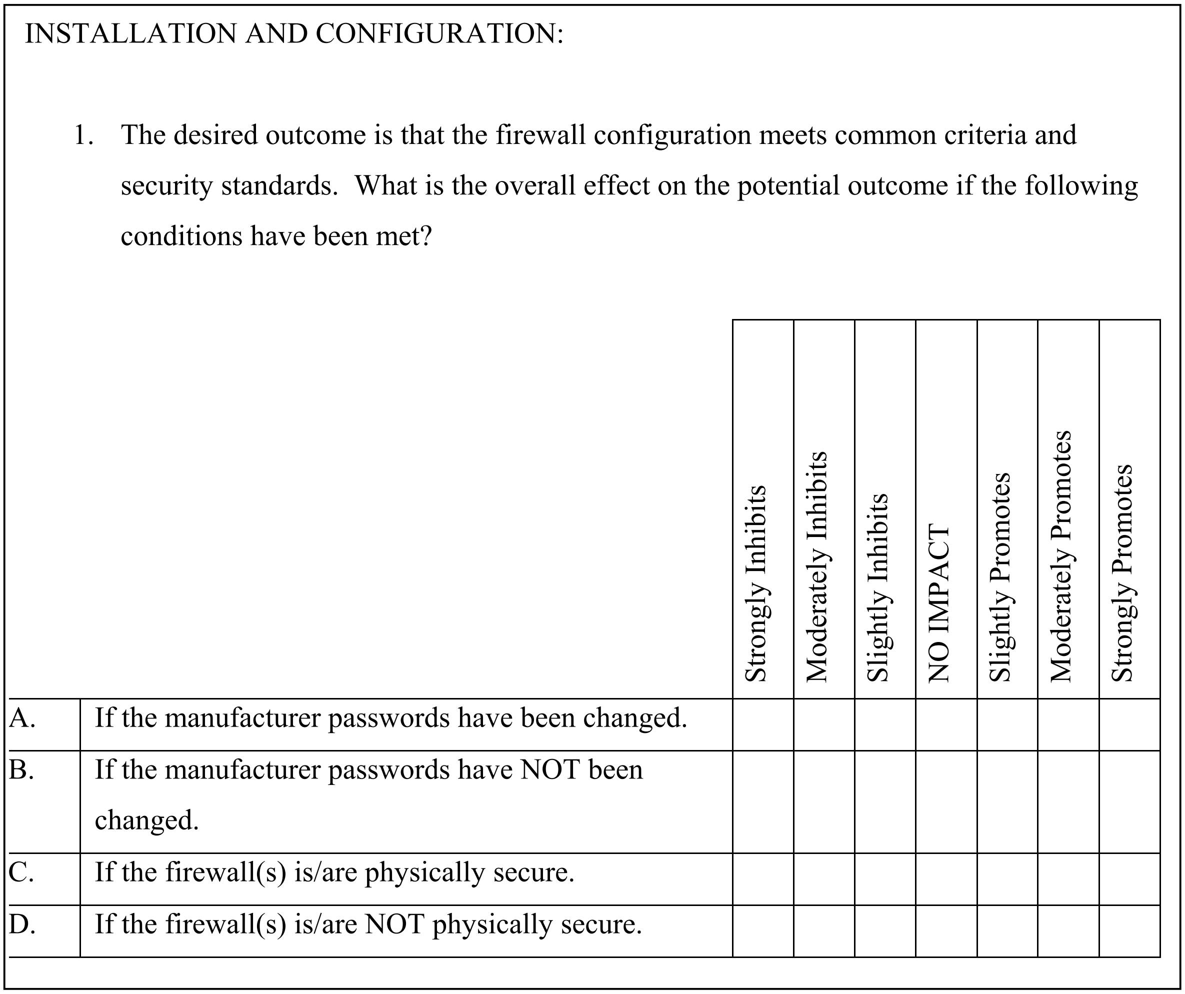
- Does the topography of the model accurately reflect the environment modeled at an intuitive level?
- Does a domain expert look at the model and consider it laughably inaccurate?

The face validity of the baseline topography was achieved during face-to-face sessions with domain experts. Without achieving face validity, even subjective calibration of the model becomes an exercise in futility. The ‘test’ amounted to an assessment of the intuitive correctness of the model based upon the accumulated expertise and knowledge of the participating people. During each session, the model met the experts’ expectations and addressed those issues considered to be important influences on IA for a firewall system.

3. Calibration

Once the initial model construction has been completed and face validity confirmed, establishing link values is the next step. This is the calibration phase. Calibration of the model applies it to a specific target environment. The model assumes the characteristics of the example. During this phase, values are assigned to both links and nodes.

Values may be set using surveys, individual interviews, collaborative processes, or some combination of the three. The surveys created in support of this thesis [Figures 11 and 12] were used in conjunction with interviews to establish the link and node values within the model for each excursion. A modified Delphi approach was used to guide the survey/interview process. A Delphi approach is one in which individual estimates are made by several raters. The estimates are then collected, reproduced and distributed to the participants. Raters are given an opportunity to modify ratings based on colleagues' input. After appropriate revisions are made, consistent values are applied and inconsistent ones are discussed further. [Pfleeger, 1997]



INSTALLATION AND CONFIGURATION:

1. The desired outcome is that the firewall configuration meets common criteria and security standards. What is the overall effect on the potential outcome if the following conditions have been met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If the manufacturer passwords have been changed.							
B.	If the manufacturer passwords have NOT been changed.							
C.	If the firewall(s) is/are physically secure.							
D.	If the firewall(s) is/are NOT physically secure.							

Figure 11: Sample from the Link Value Survey

Because SIAM provides a dynamic environment, simplifying model revisions, following a strict Delphi approach was unnecessary. The color coded visual representation and the robust analysis tools significantly enhance the ease with which a model can be tuned to most accurately represent the environment being modeled. One must be aware of what question is asked and the manner in which the question was asked. How the questions on a SIAM survey are worded, has great bearing on the validity of the results.

To begin setting the link values, one must address the statement in the child node. [Figure 11] What is the goal? Then ask the standard question: What is the overall effect on the potential outcome if the conditions have, or have not, been met? Note that the basic question is positive in nature. However, the conditions that apply are either positive and negative; either on or off. One must address both positive and negative aspects of the link on an individual basis. By posing the questions in this fashion I have found that the results do not become skewed as often happens with "check box" surveys. [Buettner, 2001]

The values set for links should reflect the ***direction*** of influence (reinforcing or reversing) parent node-to-child node and the ***degree*** (no impact to significantly impacts) to which the parent influences the child. The values for initial nodes reflect the ***level of truth*** exhibited in each statement, from compete uncertainty to certainly true or certainly false. A more detailed description of this is found in Chapter II.

INSTALLATION AND CONFIGURATION:										
		Extremely Uncertain	Very Uncertain	Reasonably Uncertain	Slightly Uncertain	COMPLETELY UNCERTAIN	Slightly Certain	Reasonably Certain	Very Certain	Extremely Certain
1.	The manufacturer passwords have been changed.									
2.	The firewall(s) is/are physically secure.									
3.	The firewall(s) are installed by Authorized									

Figure 12: Sample from the Node Value Surevey

Values for initial nodes are easily set using a straight survey. [Figure 12] One key is dividing the survey along the same lines as the initial tier of parent nodes that influence the root node. By doing so, I was able to easily group the initial nodes, thereby providing logical breaks for those completing the survey. The initial nodes should be written such that both the model and the survey make a positive statement. "Such and such HAS been done, accomplished, etc." The nodal survey addresses the relative truth of this statement. The statement either has or has not been accomplished.

Only by using both positive statements to address nodes, and by addressing link effects on a case-by-case basis, can the full power of SIAM's algorithmic engine [Chapter 2] be realized. If the modeler attempts to "game" the system by using double or triple negatives then the model will probably give the "desired" result; however, the result is often worthlessly skewed in an operational environment. In this case, ***any intuitive value inherent in the visualization within the model is lost.***

The survey technique used in this thesis provided an efficient vehicle for the rapid customization of the model to specific operational scenarios. The calibration process took between three and four hours, from start to finish (this time included survey administration and application of the results to the model), and produced analysis results that were consistent with domain expert opinion and expectations.

4. Verification

While validation of the baseline model (model without link and node values) was conducted before calibration for specific scenarios, verification is conducted after values have been added to a specific example (known as a model excursion). The verification phase is composed of an initial analysis of the model and comparison of the rough results with expert opinion. In this phase the modeler must go back to the domain area experts to ensure that the environmental model maps correctly, and that the output of the model similarly meets expectations. If there are gaps in information, then the outputs from the model will appear skewed in a manner that is not supported by the experience of experts.

The model may very well return unexpected results. However, upon further scrutiny, domain area experts often are able to come to well-reasoned, supportable conclusions as to why the model returned the result in question. [MITNOC, 2001; JIOC, 2001] Because the SIAM utilities encourage the documentation of the thought processes and reasoning put into model construction, the dynamic application environment assists in hypothesis testing.

Designed as a collaborative decision tool, SIAM supports model verification through a variety of analysis/reporting tools. The software augments a decision process when properly used. During the verification process, the robust SIAM analysis tools encourage discussion among domain experts, as well as between technicians and decision-makers, ensuring that the rationale behind links and nodes is on hand to support or refute arguments.

5. Challenges Presented

The challenges represented by this model revolve around the need for domain expert participation. Integrating the human factor is inherently challenging in any technical system. Technical systems are predictable. Humans are not. However, without human input, the relative influences of specific characteristics within the model become difficult to determine. Domain area experts provided the insight needed to determine the aspects of firewall operations important to an organization under specific conditions.

E. ANALYSIS STRATEGY

Actual analysis of the individual excursions is secondary to the proof of concept of the applicability of the model itself. When applied to specific scenarios, the model works. The findings of this thesis will be covered from two perspectives: response from the domain area experts; and excursions of the model. The model is scaleable. Excursion 1 represents an enterprise systems view while Excursion 2 exhibited a more localized organizational viewpoint.

Initial analysis of the two excursions showed results that matched the domain experts' expectations. In Excursion 1 correct installation and configuration was the function exercising the greatest influence on the root node. In Excursion 2, firewall administration held sway. The dichotomy between the two excursions demonstrates the difference in perspective between the systems engineers in Excursion 1 and the vulnerability assessment team of Excursion 2.

The following chapters will demonstrate how the model can be used to identify potential opportunities for decision-makers to make incremental investments in security, thereby increasing the overall security posture of the organization.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. EMPIRICAL FINDINGS

The previous chapter provides a detailed description of the mechanical processes used to construct, validate, calibrate, and verify the model. This chapter will focus on responses from domain area experts and a description of the excursions that were conducted.. The importance of the interview responses and implications of the successful excursion results will also be covered.

A. DOMAIN EXPERTS' RESPONSE

The modal initial response from domain experts to the thesis concept was "…it sounds like a great idea, I just don't think it can be done." The idea that one could construct a model that assisted in the prioritization of critically influential factors, in an organizational information assurance structure, was novel.

1. Methods

Domain experts were critical in the construction of this model. Informal interviews were conducted during the initial construction, validation, and verification phases; formal surveys were used in conjunction with interviews to collect data inputs during the calibration phase.

Four organizations were specifically targeted, although numerous organizations and agencies informally influenced the direction and mode of this research:

- The Marine Corps Information Technology & Network Operations Center
- The Joint Information Operations Center
- Space and Naval Warfare Systems Center, San Diego
- The National Security Agency

Each made the requisite experts within their structures available. Twenty-five domain experts, across these four organizations, were consulted over the course of this research

Although email was used to establish contacts, most of the interviews conducted were conducted in person. First-hand contact enhanced an understanding of the environment being modeled, improved the experts' understanding of the project and appeared to foster cooperation that may have increased the accuracy and intuitive correctness of the model.

2. Findings

The domain experts consulted ranged from decision-makers to vulnerability assessment specialists to systems engineers and information assurance technicians. While consensus was reached during the construction and validation phases, each of these groups brought a unique perspective to the calibration and verification phases.

In general, the groups remained true to their stereotypes: decision-makers were more concerned with administration and operations while technicians focused on the implementation of technology. The backgrounds, skill sets, and cultures of these two groups significantly influence the manner in which they approach problems and issues. Similarly, solutions are crafted upon these biases. Future research on this topic should include a solid evaluation of the obvious differences in the perspectives of these two groups.

The perspectives exhibited by the systems engineers and the vulnerability assessment specialists were extremely interesting. Given the similar backgrounds of these two groups, I expected similar responses to the model. That was not the result observed. The systems engineers focused on the installation and configuration of a firewall implementation. In contrast, the vulnerability assessment specialists considered firewall system administration to be most important. Installation and configuration was still important, but the vulnerability assessment technicians felt that systemic weaknesses could be mitigated through better administration.

The variation between the group of systems engineers and the vulnerability technicians was unexpected and counter-intuitive. Both groups have technical backgrounds. The expectation was that both groups would have similar perspectives.

Upon further consideration, the reason for the difference became apparent. The systems engineers deal with installation and configuration of hardware/software on a daily basis. Operational and administrative functions follow. The vulnerability assessment technicians deal with post installation systems. The environment assessed by this group is one in which administrative actions and operational decisions are the focus. Often the vulnerabilities identified are ones that have occurred due to administrative oversights. Bad installation and poor configurations leave systems highly vulnerable. Administrative time is consumed by patch research and application while availability degrades due to system downtime or exposure. The model improves the ability of domain experts to visualize a specific system within a common framework useful to both decision-makers and technicians.

B. MODEL EXCURSIONS

The two excursions used in this research exercise the calibration and verification phases of the development process.

1. Methods

There are three steps required to calibrate and verify the model in a specific scenario.

- Establish the link values for the model
- Populate the initial nodes
- Conduct a thumbnail analysis to ensure intuitive correctness of the model

The process used to define each excursion took three to four hours to complete.

a. Step One: Establishing Excursion Link Values

Establishing the link values within the model involves building a consensus among domain area experts on the relative influence of each parent node on its respective child node (nodes, in the case of multi-path chains). This influence is reflected in two planes: If the parent is 'true' does it reinforce (make more true) or reverse (make more false) the child node; and if the parent is 'false' does it reinforce or reverse the child node? The surveys used to establish the links values [Appendix C] addressed the parent node and relative influence for each associated child.

b. Step Two: Populating the Excursion Initial Nodes

The survey used to establish values for the initial nodes was similar to that used to establish the link values. In this instance, the survey addressed the relative certainty of each initial node. This certainty ranges from 'extremely certain' to 'extremely uncertain'. While the results are determined through background calculations on a zero-to-one range, the output is color-coded to improve intuitive recognition of the model's results. Populating the initial nodes enables the Bayesian inference net calculations to be conducted in the background. [Rosen & Smith]

c. Step Three: Conducting a thumbnail analysis

This analysis is merely an informal review of initial model results with the organization domain area experts. It supports the model verification phase described in the previous chapter. The purpose of this initial review is to ensure that the model and the output of the model mesh with the intuitive expectations of the experts. If the output varies greatly from reasonable expectations or explanation, then further analysis is required to ensure that values for links and initial nodes accurately reflect the organizational environment.

2. Findings

Gaining access to qualified domain experts qualified to provide the required data was the biggest challenge. The second challenge was asking the correct questions in the correct manner.

My experience with this research indicates that ***how*** the questions are asked is almost as important as ***what*** questions are asked with respect to establishing model validity and output viability.

By combining surveys and interviews, I found there was little confusion among participants in relation to purpose and execution, and that the resulting inputs accurately reflected reality within the systems being modeled. One set of modelers that I spoke with was attempting to use correlation analysis data collection techniques in order to establish the link values within a SIAM model. While commonly used in operations research/analysis, this technique appears to consistently skew the results of SIAM models when used to set link values. [Buettner, 2001]

I chose to administer both surveys in a collaborative environment during each excursion. An alternative is to administer the surveys to individual participants using the Delphi approach. This would require that the surveys be administered/collected, have the results tallied and then normalized, with the resulting normalized output applied to the model links. A strict Delph-based process would include a round of response revisions between the collection of the results and their tallying. This round of revisions is an opportunity for raters to change assigned values based on the inputs of their peers. While potentially less accurate, using this modified Delphi approach proved less complicated and less time consuming. A drawback of this approach is the potential for a single strong personality to dominate. In this situation it is up to the modeler, serving in the role of moderator, to drive the discussion and ensure that the process remains collaborative.

The surveys used to populate data points within a SIAM model must accurately reflect the nature and characteristics of the model itself. Attention to detail, treating the values of link strengths individually, and ensuring that initial nodes are reduced to statements about which the relative truth can be determined will assist in closely mapping the surveys to the model.

The model effectively represented the modeled environments in both excursions. In each case, the overall results paralleled the expectations of domain experts. The model did identify systemic issues and relationships that were not previously obvious.

V. BEYOND CLASSICAL RISK ANALYSIS

Risk analysis is a process undertaken to determine the exposures within a system and their potential harm. The process forces the systematic study of the exposures and assists in justifying the type or quantity of security required. [Pfleeger, 1997] Although, the purpose of the model is to support the justification of security processes or techniques, just as classical risk analysis does. This model does not conduct risk assessments in the classical sense. Rather, it expands on classical methods in order to:

- Enhance visualization of the target system.
- Provide a dynamic evaluation environment, responsive to rapidly changing information assurance requirements.
- Encourage dialog between decision-makers and technicians through the provision of a common frame of reference.

The model ***evaluates, prioritizes, and graphically illustrates shortfalls*** within two systems based on the relative importance of specific criteria as established by domain experts. It also ***facilitates the extraction of implicit or tacit knowledge*** from these same domain experts that would not emerge during classical risk analysis.

To Will Ozier, risk analysis "…represents the process of analyzing a target environment and the relationships of its risk-related attributes." [Ozier, 2000] Some benefits of conducting a careful risk analysis include:

1. Improving awareness of security issues.
2. Identification of assets, vulnerabilities, and controls.
3. Improving the basis for decisions.
4. Justifying expenditures for security.

[Pfleeger, 1997]

Using these criteria, construction and subsequent use of the model constitutes a risk analysis. The model provides a dynamic environment that inherently tracks the relative importance of factors directly and indirectly influencing the strategic security goal; classical risk analysis is inherently static.

Use of the model offers several improvements over the classical approach. The model graphically illustrates the relationships of which Ozier [2000] spoke. Additionally, the model provides a more dynamic environment. One can adjust individual criteria and generate immediate feedback on the potential systemic benefit or loss associated with the new value. The model also provides a common frame of reference for decision-makers and technicians during the evaluation process. This common picture further supports the accuracy and utility of the model in the development of a more uniform security posture. The significant benefit over classical techniques is the ability to gauge results in regards to their systemic impact on enterprise goals and objectives. This correlation is not automatic using classical risk analysis.

Risk analysis usually focuses on the risks associated with not spending money on information assurance. It focuses on what costs might be incurred based on a ***bad*** event occurring. These costs are used to calculate the return on investment for a given expenditure. Peltier states that, "The goal of risk analysis is not to eliminate all risk. It is a tool to be used by management to reduce risk to an acceptable level." [Peltier, 2001]

Classical risk analysis identifies potential threats, the potential frequency of occurrence, and the potential costs associated with a threat occurrence and the subsequent recovery. The model presented here serves as a planning tool that assists decision-makers and technicians in evaluating the current status of a target system and then prioritizing which combination of assets, procedures, and security techniques may improve (or decrease) the overall security posture in relation to the goals and objectives of the enterprise.

A. QUANTITATIVE RISK ANALYSIS

Quantitative risk analysis involves assigning numerical values to (1) monetary criteria, (2) observed percentages, (3) annualized rates of occurrence, and (4) bounded distributions. These four metrics are applied to the standard six risk elements:

- Asset value
- Threat frequency
- Threat exposure factor
- Recommended safeguard effectiveness
- Safeguard cost
- Uncertainty

[Peltier, 2001]

Benefits revolve around the numerical basis of the data and statistical analysis conducted on the data collected. Relative values of information, often expressed in monetary terms, are often better understood by decision-makers. In government and the Department of Defense, systems losses and relative values of information may be expressed in terms of value to national security, lives of personnel, or significant losses of equipment and resources. Because assessment results are generally based on monetary values, percentages, and annualized probabilities a credible basis for cost/benefit assessment is assumed and risk management performance tracked and evaluated. [Ozier, 2000] Quantitative risk analysis is particularly effective when evaluating tangible assets.

The difficulties seen with quantitative techniques are focused on the relative complexity of associated calculations and the extremely involved data collection process required to support them.

B. QUALITATIVE RISK ANALYSIS

In general, calculations in qualitative analyses are few. One characteristic commonly associated with this analysis technique is that results are essentially subjective in both process and metrics. [Ozier, 2000] Peltier states that "The qualitative methodology attempts only to prioritize the various risk elements in subjective terms."

A qualitative risk analysis can be reduced to a generic ten-step process:

1. Developing a statement of scope.
2. Selecting domain area experts to participate.
3. Identification of potential threats.
4. Prioritization of identified threats.
5. Prioritization of the impact should a threat occur.
6. Calculation of the total threat impact.
7. Identification of potential safeguards.
8. Cost-benefit analysis of potential safeguards.
9. Prioritization of safeguards.
10. Completion of the risk analysis report.

[Peltier, 2001]

The subjective nature of qualitative risk assessment makes it very useful when evaluating both tangible and intangible resources, e.g. the value of an organization's reputation would be very difficult to quantify in any meaningful manner. Savvy domain area experts are required in order to effectively and efficiently organize and assess the relative values of these assets.

C. MODEL BENEFITS

The goal of the model is to enhance communication between decision-makers and technicians. It does this by providing a justifiable, prioritized list of security actions that can potentially raise the organizational security posture. The graphical nature of the output, offering observers the opportunity to visualize relationships, is the driving factor in improving communications between these two groups.

The classical risk assessment is static. It does not provide a collaborative environment that dynamically supports enhanced communications between technicians and decision-makers. "What-if" forecasting in support of changing situations or requirements is not easily conducted using either quantitative or classical qualitative techniques.

The model, as executed in this thesis, provides this collaborative decision support in a target environment. It enhances the ability of the modeler (technician or decision-maker) executing the model to prioritize the key influential actions (based on organizational priorities) within a specific implementation. Moreover, it enhances the modeler's ability to ***game*** potential outcomes in an effort to determine what will best serve the strategic goals and core processes of the organization. By adjusting the values of initial nodes or link strengths, a modeler can project what the influence may be of positive or negative changes within the target environment.

Classical risk analysis is recommended, like strategic plans, to be re-evaluated on an annual basis. This process is involved, and labor intensive. The SIAM model created during this research requires a level of effort similar to classical risk analysis methods initially. However, once the baseline model for an organization has been established, the model provides an inherently dynamic environment. Follow-on maintenance and re-calibration of the model to ensure accurate representation of the modeled environment is significantly easier. Re-evaluation of the system and re-prioritization of potential expenditures can be conducted each time system modifications or updates are made, new potential threats or safeguards are identified, or as enterprise goals and objectives change.

The model can cut the time, effort, and financial resources required to conduct periodic system evaluations and assist in projecting future expenditures most likely to contribute to a higher overall enterprise security posture. The reduction in required resources exceeds 50%.

Individual attributes can be adjusted or updated and the relative influences automatically recalculated. Additionally, sequential updates can be captured as separate excursions and compared using SIAM's cross-excursion analysis utility. Although challenging to construct, the flexibility of the model and particularly its ease of use are its greatest assets.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS AND RECOMMENDATIONS

If a strategic goal is articulated and a series of objectives or processes influencing the achievement of that goal defined, then a SIAM model may be applied as a potential solution. The model constructed as a result of this research provides a tool that is generic enough to be widely applicable and specific enough to offer utility as a communications aid to be used between decision-makers and technicians.

The model developed during this research increases visualization of the environment of a system. It provides a dynamic environment for comparative analysis of system attributes and it encourages more focused communications between decision-makers and technicians. This combination of characteristics makes it unique.

The model possesses a range of utility; from comparative base lining (current or future states relative to extant policies, goals, and objectives) to performance evaluations of internal or external agencies.

A. UTILITY OF THE APPLICATION

This model significantly improves the ability of decision-makers and technicians to develop a common frame of reference within a dynamic environment. Without this common frame of reference, decision-makers will continue to allocate resources on an ad hoc basis leaving (potentially expensive) vulnerabilities un-addressed.

1. Comparative Base Lining Relative to Stated Policy and Goals

The model can be used to develop a baseline assessment of a specific information resource security environment in relation to the stated policies, goals and objectives of an enterprise.

2. Comparison of Current States to Baselines

The flexibility of SIAM's sensitivity analysis tools enables the effective side-by-side comparison of specific states against baselines. Cross-excursion analysis [Rosen and Smith, 1999] supports comparisons within single systems, the current states of multiple systems, and current states against multiple futures.

3. Comparison of Alternatives

What is the most critical factor when considering incremental investment to achieve exponential increases in security posture? Where can an organization achieve the greatest returns on investment?

These are critical questions when considering how to allocate increasingly scarce resources. Using the model, alternative futures can be compared in pursuit of a more secure security posture. The evaluation tools available within SIAM assist in prioritizing the factors exercising the greatest influence over the modeled system such that a determination can be made concerning potential returns on investments in security solutions.

4. Evaluation of Relative Performance Levels for Internal or External Agencies

Just as current states can be compared against baselines or a comparison of alternatives made, so too can relative performance evaluations of internal or external agencies be conducted. The ability to evaluate technical performance relative to established metrics is common in many tools. However, there are no automated tools currently in existence that allow for the effective comparison of relative performance levels that include non-metric based factors. Evaluating an organization based on packets passed or intrusions deflected is common.

B. RECOMMENDATIONS FOR DOD

There are two specific applications of this tool that apply to the DoD:

1. The renovation of the Defense Information Technology Security Certification and Accreditation Process (DITSCAP).
2. The evaluation of Service Level Agreement compliance by the prime and sub-contractors on the Navy-Marine Corps Intranet (NMCI).

1. Comparative Base Lining in Support of Certification and Accreditation

The DITSCAP is a static evaluation process used to determine organizational preparedness to function securely in an information technology intensive environment. The process is used to evaluate organizations, their hardware and software, and their operational facilities. The certification and accreditation process is mandatory for any organization desiring connections with the Defense Information Services Network (DISN).

Although currently focused on firewall issues, the model generated by this research can be modified and expanded to cover all of the topics resident in the DITSCAP. The establishment of relational links between evaluation criteria will greatly enhance the realistic representation of the modeled environment during the evaluation. Additionally, the model provides a dynamic, easily maintained, environment within which an evaluation can be conducted or updated. A single attribute can be modified and an update of the model conducted immediately. This level of control has the potential to free up significant manpower when compared to the current system.

2. Performance Base-lining and Comparative Evaluation

The NMCI contract currently allows for a bonus incentive structure in addition to the straight fee-for-service cost structure. The bonuses are paid according to the level of compliance with the Service Level Agreements (SLAs) upon which the contract is based. In most cases the evaluation of this compliance relies on technical metrics (packets passed successfully, intruders detected/thwarted, etc.). **There is no mechanism currently in place that supports evaluation of performance levels in relation to the stated policies, goals, and objectives of the NMCI. [DON CIO]**

A permutation of the model can evaluate the relative success or failure of the prime and sub-contractors in achieving the specified goals and objectives. This evaluation would graphically illustrate the degree to which the SLAs had been achieved thereby giving the government and the vendors common ground for discussion of fee-for-service issues as well as full or partial bonus incentives.

A model agreed upon by both parties to the contract supports a common dialog. Such a model provides the government with an evaluative tool that may save unjustified incentives, and provides the vendor with a vehicle to argue in favor of bonus incentives for meeting specified levels of performance.

C. FUTURE RESEARCH

1. Integration of the Model into the DITSCAP Process

This modeling technique can be integrated into the DITSCAP process. Future research in this area should focus on constructing a dynamic model to be used in place of the current DITSCAP checklist. The model should evaluate the holistic status of a given enterprise and its relative security posture.

Integration of the model into the DITSCAP process will entail a significant expansion of its existing boundaries. Instead of focusing solely on firewalls, a model evaluating DITSCAP-esque requirements must encompass a full range of information assurance issues. Although this will require an investment in human capital up front, the creation of a dynamic environment and supporting historical models has the potential to significantly decrease manpower requirements during DITSCAP evaluations and reviews over the long term.

2. Expansion of the Model to Evaluate SLA Compliance in Support of NMCI

There are thirty-eight SLAs supporting the NMCI contract vehicle. [NMCI, 2000] Although not necessarily applicable to all of them, the model can make significant contributions to the SLA evaluation process. Future study in this area should define which SLAs are appropriate for application of the model and then construct a set of evaluative models. These sub-models should be constructed with the idea of integrating them into an over-arching NMCI model that could be used to provide an effective evaluation of overall program status.

D. CONCLUSION

A baseline model was constructed and validated by a group of domain experts. Test cases (excursions within the model) were run successfully and also found to meet the expectations of the experts. Improvements and renovations were applied as a result of consultation and interviews with the domain experts. These modifications enhanced the capabilities of the model in both form and function. Lastly, a comparison was drawn between the model (and supporting processes) and the processes used during classical risk analysis.

The model presented in this thesis represents a mere sliver of the previously unexplored potential that the Situational Influence Assessment Module offers in this field. A dynamic environment has been created that enhances the visualization of complex information assurance relationships between technical implementations and their impacts on strategic goals and policy. By applying this modeling process in an information assurance environment, decision-makers and technicians have an opportunity to leverage a common framework. In doing so, both groups gain the ability to communicate more effectively and allocate scarce resources more efficiently.

APPENDIX A. FIREWALLS DESCRIBED

"…If it's supposed to keep the bad guys out of your network, it's a firewall. If it succeeds in keeping the bad guys out, while still letting you happily use your network, it's a good firewall; if it doesn't, it's a bad firewall." [Zwicky, et.al., 2000]

A. OVERVIEW

Firewalls are tools used in securing a network from hostile intrusion. However, they have weaknesses. Inattentive configuration, insufficient physical security, inappropriate rule sets, and overly ambitious expectations (born of the panacea that once a firewall is installed and organization is secure) all contribute to firewall failures. As this appendix is provided as a broad-brush overview, the references provide a wealth of detailed information on firewalls, their strengths and weaknesses.

Firewalls can be many things: hardware, software, or a combination of the two. They are often thought to be the panacea for information assurance in a networked environment: perfect gateways keeping all of the miscreants out, and allowing all authorized users perfect access; bastions of security firmly entrenched at the front door of the enterprise. "People expect a firewall to be a solid brick wall protecting some computing resources." [Pfleeger, 1997]

1. What is a Firewall?

Firewalls have been defined in as many different ways as there are products. A firewall is:

"A process that filters all traffic between a protected or 'inside' network and a less trustworthy or 'outside' network"; [Pfleeger, 1997]

"Any security system protecting the boundary of an internal network"; [Gollman, 1999]

"A network monitor or collection of monitors placed between an organization's internal network and the Internet or between two local area networks (LANs)"; [Denning, 1999a]

"A system or group of systems that enforces an access control policy on network traffic as it passes through access points." [Brenton, et al., 2001]

The definition preferred for this thesis is: a firewall "…is a system of components designed to control access to and from your network and an external network, based on the security policies in effect at your site." [Ogletree, 2000]

2. Defining an Access Control Policy

An access control policy is "…simply a corporate policy that states which type of access is allowed across an organization's network perimeters." [Brenton, et al., 2001]

Access control policies may cover many different areas within an organization. They may limit the scope of access for authorized users; the types of data that may be passed or blocked; or specify data flow direction.

Access control policies take on two flavors: Default Deny; and Default Permit.

a. Default Deny Stance

That which is not expressly permitted is prohibited. This is the fail-safe posture in the information assurance environment. This posture "…recognizes that what you don't know *can* hurt you." [Zwicky, et al., 2000]

Allowed services are specified and all other traffic is denied. By enabling services on a case-by-case basis only, authorized personnel can examine the services users want; consider the security implications of providing the desired services; and allow only those services that support the mission, core processes, and security objectives of the enterprise.

b. Default Permit Stance

That which is not expressly prohibited is permitted. Laissaiz-faire network management. In this case, all actions are permitted unless they have been specifically denied.

There is a critical weakness inherent in this policy stance: "Trying to guess what dangers might be in a system or out there on the Internet is essentially an impossible task." [Zwicky, et al., 2000] This posture tends to degenerate into a sprint between systems administrators (to increase security) and users (figuring out cool new ways to do things they are not supposed to be doing).

B. FIREWALL EFFECTIVENESS

Firewall effectiveness revolves around conscientious and effective installation and configuration, and regular maintenance and administration. Firewalls are most effective when employed as a component within a defense-in-depth security solution. Firewalls cannot be installed and then summarily forgotten.

1. Capabilities

As stated previously, firewalls are not a panacea to be indiscriminately strewn around a network. They represent a solid security component that, for the uninformed, can quickly contribute to an immensely false sense of security. The attitude that **we have a firewall, therefore we must be secure** is prevalent at all levels of many organizations.

In general, firewalls can offer the following benefits:

- Protection from insecure protocols and services.
- Keeping information about…your network from prying eyes outside your network.
- Provides audit trails.
- Provides centralized management of network security as it relates to the outside world.

[Ogletree, 2000]

2. Limitations

The biggest limitation of firewalls is that they will not protect an organization from an inside job. No matter how secure the firewall installation may be, an authorized user on the inside of the boundary layer can potentially cause significant harm to the enterprise network. Insider attacks are a very real threat. Ogletree [2000] comes to the point with his statement that, "A firewall is not a substitute for everyday system management and security measures."

Zwicky, *et al.* [2000] provides a quick, concise list of what firewalls *CANNOT* do:

- Protect against malicious insiders.
- Protect against connections that do not go through them.
- Protect against completely new threats.
- Set themselves up correctly.

Some other issues that firewalls cannot, in and of themselves, completely defend against are: viruses; Trojan horses; social engineering; physical outages; and user/administrator incompetence. These limitations, inherent in a firewall system, can be mitigated by:

1. Proactively keeping patches up to date;
2. Ensuring system configurations are well documented;
3. Taking advantage of available training for users as well as administrators;

4. And, effectively communicating with users.

[Schultz, 2000]

C. DECOMPOSITION OF A TECHNOLOGY CLASS

Firewalls as a class of technology have some common features. In general, all firewalls are designed to perform a border security function, acting as a single point of entry and exit for traffic on the network. They examine network data in transit, based on a set of pre-defined criteria, and either pass or drop the data packets as determined by the rule set.

Firewall functionality is comprised of three fundamental capabilities:

1. Packet Filtering: Passing or dropping packets based on characteristics of header information;
2. Network Address Translation: Converting internal IP addresses to addresses based on the firewall in order to conceal them from external monitoring (also called IP masquerading);
3. Proxy Services: Application layer connections designed to break the network layer connection between internal and external hosts.

[Strebe & Perkins, 2000]

There are several different types of firewalls, each with unique functional characteristics. Simple packet filters, application gateways or proxy servers, and hybrid systems all serve these same basic functions. The primary differences are found in *how* these basic functions are performed and what extended features are available.

1. Packet Filtering Firewalls

Packet filters offer relatively minimum security, but do so at a relatively low cost. The biggest advantage of packet filters is that they are fast, flexible and transparent. [Blanding, 2000] There are two types of packet filters: static and dynamic. Both operate at the network transport layer (layer three of the OSI model). [Brenton, 2001] Firewalls with static packet filtering are the simplest and most common. They compare "…network protocols (such as IP) and transport protocols (such as TCP) to a database of rules and forward only those packets that conform to the criteria specified in the database of rules." [Strebe & Perkins, 2000] The firewall either passes or drops the examined packet. These firewalls are stateless, there is no record of the network session connection or the examined packet after disposition has been made with this type of firewall.

The dynamic packet filter maintains the state of the connection with a record of the communications session for each packet. If an inbound packet does not contain a request to open a session or a response to a recorded outbound request, then, if the system is configured for default denial of access the packet or packets are dropped automatically. Inbound and outbound packets can also be screened according to network or transport protocols, origin, destination, etc. A dynamic filter can be expanded further to include stateful filtering. In this type of filter, rules are protocol specific and track session context as well as the states represented in a connection table. [Brenton & Hunt, 2001]

Packet filters are limited to examining the packet header information. These firewalls offer only limited security and should be used as a first line of defense in a defense-in-depth scenario in all but the least secure of environments.

Packet filters can be deployed very effectively as *gatekeepers* on reasonably secure networks. The packet filter is commonly implemented as a front for a dual-homed host, a screened-host configuration, or a screened subnet. [Strebe & Perkins, 2000] Each configuration offers its own strengths and weaknesses.

2. Application Gateways / Proxy Servers

Application gateways or proxy servers operate at the application layer (layer seven) of the OSI model. The primary difference between packet filters and proxies is that the "…proxy server must understand the application." [Strebe & Perkins, 2000] This means that the proxy server is application specific. This specificity allows for great flexibility in configuring the firewall---individual application services can be passed or denied.

The proxy server also serves as a *middleman* between applications and user service requests. In this role, user requests never reach the destination application. Rather, the request goes to the application gateway. The gateway translates and forwards the request (based on the applicable rule set and using its own IP address as the source address) to the specified service. The proxy then receives the response from the service provider as if it was the original requester. The response is forwarded (again examining the data given the rule set parameters and using its own address as the source address) back to the requesting user.

The proxy server creates new data packets for both inbound and outbound transmissions. As such, the proxy represents a dual identity: To the user the proxy server is the provider of the requested service; to the service provider, the proxy is the original requester. This process is bi-directional. [Strebe & Perkins, 2000]

3. Hybrids

Hybrid systems combine the characteristics of packet filters and proxy servers into a single device. The downside is the inherited set of weaknesses from both systems. A more secure option is to deploy packet filters and proxy servers in mutually supporting configurations such as: a dual-homed or bastion host; screened hosts, or screened subnets. [Goncalves, 2000]

APPENDIX B. EXCURSION ONE

The surveys in this appendix do not represent evaluations of production network systems, rather the collective experience and compiled opinions of the domain experts surveyed.

A. MARINE CORPS INFORMATION TECHNOLOGY & NETWORK OPERATIONS CENTER

The Link Surveys were created in support of the modeling effort as described in chapters two and three. The link value surveys for each excursion are listed below.

1. Link Value Survey

The following is a survey designed to collect data on the relative values of link strengths within the SIAM model. Completion of the survey should take approximately 45 minutes. This survey may be completed by typing directly into this document and emailing the file back to mailto:cpbrodhu@nps.navy.mil; or the survey may be completed in hard copy and faxed back to Major Brodhun, Code 32, NPGS, at (831) 656-3681 / DSN 878-4656.

Please fill in the required reference data.

COMMAND: Marine Corps Information Technology & Network Operations Center
CONTACT INFO--Phone: ________________ Email: ________________________

You will see desired outcomes listed below. Sets of potential conditions are listed in tables underneath each outcome. Place an "X" in the column to the right, which most accurately reflects the relative influence of each event on the desired outcome. This survey is NOT concerned with the existence or non-existence of the listed conditions in a specific implementation. Rather, this survey is addressing the RELATIVE IMPACT of the condition on the outcome if the condition did or did NOT exist.

INSTALLATION AND CONFIGURATION:

1. The desired outcome is that the firewall configuration meets common criteria and security standards. What is the overall effect on the potential outcome if the following conditions have been met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If the manufacturer passwords have been changed.							X
B.	If the manufacturer passwords have NOT been changed.	X						
C.	If the firewall(s) is/are physically secure.							X
D.	If the firewall(s) is/are NOT physically secure.	X						
E.	If the firewall(s) are installed by Authorized Personnel only.							X
F.	If the firewall(s) are NOT installed by Authorized Personnel.	X						
G.	If the firewall rule-set has been well defined.						X	
H.	If the firewall rule-set has NOT been well defined.		X					
I.	If the allowed and disallowed services have been specifically defined.							X
J.	If the allowed and disallowed services have NOT been specifically defined.	X						
K.	If the firewall(s) are supported by a secure network infrastucture.						X	
L.	If the firewall(s) are NOT supported by a secure network infrastucture.		X					
M.	If the firewall configurations allow for automated fail-over capabilities.							X
N.	If the firewall configurations DO NOT allow for automated fail-over capabilities.	X						

2. The desired outcome is to have the firewall rule set be well defined in its initial state. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If a split DNS has been implemented.					X		
B.	If a split DNS has NOT been implemented.			X				
C.	If specific services have been defined as “allowed.”							X
D.	If specific services have NOT been defined as “allowed.”	X						
E.	If specific services have been defined as “denied.”					X		
F.	If specific services have NOT been defined as “denied.”			X				
G.	If the “direction of flow” for each allowed and denied service has been determined and set.							X
H.	If the “direction of flow” for each allowed and denied service has NOT been set.	X						

3. The desired outcome is to have the services that are allowed and NOT allowed to pass through the firewall(s) to be specifically defined. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If services have been specifically defined as "allowed."							X
B.	If services have NOT been specifically defined as being "allowed."	X						
C.	If services have been specifically defined as "denied."					X		
D.	If services have NOT been specifically defined as "denied."			X				

4. The desired outcome is to have a stable and mature operating system supporting the firewall. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If the operating system supporting the firewall has been fully tested and patched (i.e., the OS is current).							X
B.	If the firewall operating system has NOT been fully vetted and patched.	X						
C..	If the IP Stack configurations are protected.							X
D.	If the IP Stack configurations have NOT been protected.	X						
E.	If the OS feature set is known and well documented.							X
F.	If the OS feature set is NOT well known.	X						
G.	If the OS allows system configuration by users.		X					
H.	If the OS does NOT allow system configuration by users.					X		

5. The desired outcome is to have a firewall implementation supported by a secure infrastructure. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If infrastructure power is clean and protected within Enterprise boundaries.						X	
B.	If infrastructure power is NOT clean (i.e. subject to spikes and brown-outs) and NOT protected within the enterprise.	X						
C.	If emergency power is available in case of an infrastructure failure.							X
D.	If emergency power is NOT available in case of an infrastructure failure.	X						

6. The desired outcome is to have a firewall configuration that allows an automated fail-over capability. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If firewalls are installed in pairs to maintain a redundant architecture.							X
B.	If firewalls are NOT installed in pairs (thereby introducing a single point of failure).	X						

ADMINISTRATION AND OPERATIONS:

7. The desired outcome is to have a firewall implementation correctly installed and efficiently utilized. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If the firewall implementation configuration meets accepted common criteria and security standards.							X
B.	If the firewall implementation configuration does NOT meet accepted common criteria and security standards.	X						
C.	If administrative procedures are effective.							X
D.	If administrative procedures are NOT effective.		X					
E.	If operational procedures are effective.							X
F.	If operational procedures are NOT effective.		X					

8. The desired outcome is that operational procedures are effective in supporting the security of the firewall implementation. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If the operational requirements of the organization (requirements levied on the system) have been well and correctly defined.							X
B.	If the operational requirements of the organization (requirements levied on the system) have NOT been well defined.	X						
C.	If procedures are in place to aid in Incident Recovery.							X
D.	If procedures are NOT in place to aid in Incident Recovery.	X						
E.	If the traffic flow is closely monitored.						X	
F.	If the traffic flow is NOT closely monitored.			X				
G.	If the firewall is impairing network throughput.				X			
F.	If the firewall is NOT impairing network throughput.				X			

9. The desired outcome is that the throughput requirements are being met. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If the operational requirements of the organization (requirements levied on the system) have been well defined.				X			
B.	If the operational requirements of the organization (requirements levied on the system) have NOT been well defined.				X			
C.	If the minimum throughput requirements have been defined.							X
D.	If the minimum throughput requirements have NOT been defined.	X						

10. The desired outcome is that procedures are put in place to aid in Incident Recovery. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If incident response and reporting procedures are in place.							X
B.	If incident response and reporting procedures are NOT in place.	X						
C.	If disaster recovery procedures are defined.							X
D.	If disaster recovery procedures are NOT defined.	X						
E.	If disaster recovery procedures have been disseminated to authorized personnel.							X
F.	If disaster recovery procedures have NOT been disseminated to authorized personnel.	X						

11. The desired outcome is that incident response and reporting procedures are in place and utilized. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If automated intrusion detection and reporting is implemented at the boundary layer.						X	
B.	If automated intrusion detection and reporting is NOT implemented at the boundary layer.			X				
C.	If automated intrusion response has been implemented.							X
D.	If automated intrusion response has NOT been implemented.	X						
E.	If dynamic recovery and fail-over capabilities have been implemented.						X	
F.	If dynamic recovery and fail-over capabilities have NOT been implemented.		X					
G.	If penetration testing is periodically conducted.					X		
H.	If penetration testing is NOT periodically conducted.			X				

12. The desired outcome is that disaster recovery procedures have been put in place. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If dynamic recovery and fail-over capabilities have been implemented.						X	
B.	If dynamic recovery and fail-over capabilities have NOT been implemented.	X						
C.	If backups of configuration files and firewall rule sets are maintained.							X
D.	If backups of configuration files and firewall rule sets are NOT maintained.	X						

13. The desired outcome is to have the system traffic flow be carefully monitored. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If the minimum throughput requirements have been defined.						X	
B.	If the minimum throughput requirements have NOT been defined.			X				
C.	If content scanning is effectively conducted at the boundary layer.							X
D.	If content scanning is NOT effectively conducted at the boundary layer.	X						
E.	If mail filtering is conducted at the boundary layer.							X
F.	If mail filtering is NOT conducted at the boundary layer.		X					
G.	If packet fragments are cued, reassembled, and inspected at the boundary layer.							X
H.	If fragmented packets are NOT cued, reassembled, and inspected at the boundary layer.	X						

14. The desired outcome is that proactive management and auditing is conducted. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If active operational management techniques are employed.							X
B.	If active operational management techniques are NOT employed.	X						
C..	If rule sets are effectively documented and managed.							X
D.	If rule sets are NOT effectively documented and managed.	X						
E..	If logs are incorporated into the overall audit architecture.						X	
F.	If logs are NOT incorporated into the overall audit architecture.		X					
G..	If trend analysis is conducted on audit and intrusion detection logs.						X	
H.	If trend analysis is NOT conducted on audit and intrusion detection logs.			X				
I.	If patches and updates are kept current.							X
J.	If patches and updates are NOT kept current.	X						

15. The desired outcome is that active, operational management techniques are employed. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If content scanning is effectively conducted at the boundary layer.							X
B.	If content scanning is NOT effectively conducted at the boundary layer.	X						
C.	If mail filtering is conducted at the boundary layer.							X
D.	If mail filtering is NOT conducted at the boundary layer.	X						
E.	If packet fragments are cued, reassembled, and inspected at the boundary layer.							X
F.	If fragmented packets are NOT cued, reassembled, and inspected at the boundary layer.	X						
E.	If automated data logging procedures have been put in place.							X
F.	If automated data logging procedures have NOT been put in place.	X						

16. The desired outcome is to have procedures put in place that will support recovery from change. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If backups of configuration files and rule sets are maintained.							X
B.	If backups of configuration files and rule sets are NOT maintained.	X						
C.	If configuration criteria and standards are reviewed periodically.						X	
D.	If configuration criteria and standards are NOT reviewed periodically.			X				
E.	If remote access control lists are maintained and closely monitored.							X
F.	If remote access control lists are NOT maintained and closely monitored.	X						

17. The desired outcome is to have rule sets be completely documented and effectively managed. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If backups of configuration files and rule sets are maintained.						X	
B.	If backups of configuration files and rule sets are NOT maintained.	X						
C.	If rules changes are evaluated to determine their security impact.							X
D.	If rules changes are NOT evaluated to determine their security impact.	X						
E.	If rules changes are fully justified and completely documented.							X
F.	If rules changes are NOT fully justified and completely documented.	X						
G.	If rules sets are administered by authorized personnel only.							X
H.	If rules sets are NOT administered strictly by authorized personnel.	X						

2. Node Value Survey for the Marine Corps Information Technology & Network Operations Center

The following is a survey designed to collect data on the relative values of nodal values within the SIAM model. Completion of the survey should take approximately 45 minutes. This survey may be completed by typing directly into this document and emailing the file back to mailto:cpbrodhu@nps.navy.mil; or the survey may be completed in hard copy and faxed back to Major Brodhun, Code 32, NPGS, at (831) 656-3681 / DSN 878-4656.

COMMAND: Marine Corps Information Technology & Network Operations Center

You will see desired outcomes listed below. Sets of potential conditions are listed in tables underneath each outcome. Place an "X" in the column to the right, which most accurately reflects the relative influence of each event on the desired outcome. This survey is NOT concerned with the existence or non-existence of the listed conditions in a specific implementation. Rather, this survey is addressing the RELATIVE TRUTH of the event.

INSTALLATION AND CONFIGURATION:

		Extremely Uncertain	Very Uncertain	Reasonably Uncertain	Slightly Uncertain	COMPLETELY UNCERTAIN	Slightly Certain	Reasonably Certain	Very Certain	Extremely Certain
1.	The manufacturer passwords have been changed.									X
2.	The firewall(s) is/are physically secure.									X
3.	The firewall(s) are installed by Authorized Personnel only.									X

		Extremely Uncertain	Very Uncertain	Reasonably Uncertain	Slightly Uncertain	COMPLETELY UNCERTAIN	Slightly Certain	Reasonably Certain	Very Certain	Extremely Certain
4.	The “direction of flow” for each allowed and denied service has been determined and set.								X	
5.	A split DNS has been implemented.									X
6.	Specific services have been defined as “allowed.”								X	
7.	Specific services have been defined as “denied.”						X			
8.	The operating system supporting the firewall has been fully tested and patched (i.e., the OS is current).							X		
9.	The firewall(s) are supported by a secure network infrastructure.								X	
10.	The OS allows system configuration by users.				X					
11..	The OS feature set is known and well documented.							X		
12.	The IP Stack configurations are protected.							X		
13.	The firewall configurations allow for automated fail-over capabilities.								X	
14.	The infrastructure power is clean and protected within Enterprise boundaries.						X			
15.	The emergency power is available in case of an infrastructure failure.						X			
16.	The firewalls are installed in pairs to maintain a redundant architecture.						X			

ADMINISTRATION AND OPERATIONS:

		Extremely Uncertain	Very Uncertain	Reasonably Uncertain	Slightly Uncertain	COMPLETELY UNCERTAIN	Slightly Certain	Reasonably Certain	Very Certain	Extremely Certain
1.	The operational requirements of the organization (requirements levied on the system) have been well defined.									X
2.	The minimum throughput requirements have been defined.				X					
3.	Content scanning is effectively conducted at the boundary layer.			X						
4.	Mail filtering is conducted at the boundary layer.							X		
5.	Packet fragments are cued, reassembled, and inspected at the boundary layer.				X					
6.	Automated data logging procedures have been put in place.								X	
7.	Penetration testing is periodically conducted.						X			
8.	Automated intrusion detection and reporting is implemented at the boundary layer.								X	
9.	Automated intrusion response has been implemented.				X					
10.	Dynamic recovery and fail-over capabilities have been implemented..						X			
11.	Backups of configuration files and firewall rule sets are maintained.						X			

		Extremely Uncertain	Very Uncertain	Reasonably Uncertain	Slightly Uncertain	COMPLETELY UNCERTAIN	Slightly Certain	Reasonably Certain	Very Certain	Extremely Certain
12.	Rules changes are evaluated to determine their security impact.				X					
13.	Rules changes are fully justified and completely documented.						X			
14.	Rules sets are administered by authorized personnel only.									X
15.	Configuration criteria and standards are reviewed periodically.								X	
16.	Remote access control lists are maintained and closely monitored.									X
17.	Patches and updates are kept current.							X		
18.	Trend analysis is conducted on audit and intrusion detection logs.						X			
19.	Logs are incorporated into the overall audit architecture.							X		

APPENDIX C. EXCURSION TWO

The surveys in this appendix do not represent evaluations of production network systems, rather the collective experience and compiled opinions of the domain experts surveyed.

A. JOINT INFORMATION OPERATIONS CENTER

1. Link Value Survey

The following is a survey designed to collect data on the relative values of link strengths within the SIAM model. Completion of the survey should take approximately 45 minutes. This survey may be completed by typing directly into this document and emailing the file back to mailto:cpbrodhu@nps.navy.mil; or the survey may be completed in hard copy and faxed back to Major Brodhun, Code 32, NPGS, at (831) 656-3681 / DSN 878-4656.

COMMAND: Joint Information Operations Center

You will see desired outcomes listed below. Sets of potential conditions are listed in tables underneath each outcome. Place an "X" in the column to the right, which most accurately reflects the relative influence of each event on the desired outcome. This survey is NOT concerned with the existence or non-existence of the listed conditions in a specific implementation. Rather, this survey is addressing the RELATIVE IMPACT of the condition on the outcome if the condition did or did NOT exist.

INSTALLATION AND CONFIGURATION:

1. The desired outcome is that the firewall configuration meets common criteria and security standards. What is the overall effect on the potential outcome if the following conditions have been met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If the manufacturer passwords have been changed.							X
B.	If the manufacturer passwords have NOT been changed.		X					
C.	If the firewall(s) is/are physically secure.						X	
D.	If the firewall(s) is/are NOT physically secure.			X				
E.	If the firewall(s) are installed by Authorized Personnel only.							X
F.	If the firewall(s) are NOT installed by Authorized Personnel.			X				
G.	If the firewall rule-set has been well defined.							X
H.	If the firewall rule-set has NOT been well defined.	X						
I.	If the allowed and disallowed services have been specifically defined.						X	
J.	If the allowed and disallowed services have NOT been specifically defined.		X					
K.	If the firewall(s) are supported by a secure network infrastucture.							X
L.	If the firewall(s) are NOT supported by a secure network infrastucture.	X						
M.	If the firewall configurations allow for automated fail-over capabilities.					X		
N.	If the firewall configurations DO NOT allow for automated fail-over capabilities.				X			

2. The desired outcome is to have the firewall rule set be well defined in its initial state. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If a split DNS has been implemented.					X		
B.	If a split DNS has NOT been implemented.			X				
C.	If specific services have been defined as “allowed.”					X		
D.	If specific services have NOT been defined as “allowed.”				X			
E.	If specific services have been defined as “denied.”						X	
F.	If specific services have NOT been defined as “denied.”.	X						
G.	If the “direction of flow” for each allowed and denied service has been determined and set..					X		
H.	If the “direction of flow” for each allowed and denied service has NOT been set.		X					

3. The desired outcome is to have the services that are allowed and NOT allowed to pass through the firewall(s) to be specifically defined. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If services have been specifically defined as "allowed."					X		
B.	If services have NOT been specifically defined as being "allowed."				X			
C.	If services have been specifically defined as "denied."							X
D.	If services have NOT been specifically defined as "denied."		X					

4. The desired outcome is to have a stable and mature operating system supporting the firewall. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If the operating system supporting the firewall has been fully tested and patched (i.e., the OS is current).							X
B.	If the firewall operating system has NOT been fully vetted and patched.		X					
C.	If the IP Stack configurations are protected.					X		
D.	If the IP Stack configurations have NOT been protected.			X				
E.	If the OS feature set is known and well documented.						X	
F.	If the OS feature set is NOT well known.			X				
G.	If the OS allows system configuration by users.					X		
H.	If the OS does NOT allow system configuration by users.		X					

5. The desired outcome is to have a firewall implementation supported by a secure infrastructure. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If infrastructure power is clean and protected within Enterprise boundaries.					X		
B.	If infrastructure power is NOT clean (i.e. subject to spikes and brown-outs) and NOT protected within the enterprise.			X				
C.	If emergency power is available in case of an infrastructure failure.					X		
D.	If emergency power is NOT available in case of an infrastructure failure.				X			

6. The desired outcome is to have a firewall configuration that allows an automated fail-over capability. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If firewalls are installed in pairs to maintain a redundant architecture.						X	
B.	If firewalls are NOT installed in pairs (thereby introducing a single point of failure).			X				

ADMINISTRATION AND OPERATIONS:

7. The desired outcome is to have a firewall implementation correctly installed and efficiently utilized. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If the firewall implementation configuration meets accepted common criteria and security standards.							X
B.	If the firewall implementation configuration does NOT meet accepted common criteria and security standards.		X					
C.	If administrative procedures are effective.							X
D.	If administrative procedures are NOT effective.	X						
E.	If operational procedures are effective.							X
F.	If operational procedures are NOT effective.	X						

8. The desired outcome is that operational procedures are effective in supporting the security of the firewall implementation. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If the operational requirements of the organization (requirements levied on the system) have been well and correctly defined.							X
B.	If the operational requirements of the organization (requirements levied on the system) have NOT been well defined.		X					
C.	If procedures are in place to aid in Incident Recovery.						X	
D.	If procedures are NOT in place to aid in Incident Recovery.			X				
E.	If the traffic flow is closely monitored.					X		
F.	If the traffic flow is NOT closely monitored.			X				
G.	If the firewall is impairing network throughput.		X					
F.	If the firewall is NOT impairing network throughput.						X	

9. The desired outcome is that the throughput requirements are being met. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If the operational requirements of the organization (requirements levied on the system) have been well defined.						X	
B.	If the operational requirements of the organization (requirements levied on the system) have NOT been well defined.			X				
C.	If the minimum throughput requirements have been defined.						X	
D.	If the minimum throughput requirements have NOT been defined.			X				

10. The desired outcome is that procedures are put in place to aid in Incident Recovery. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If incident response and reporting procedures are in place.							X
B.	If incident response and reporting procedures are NOT in place.	X						
C.	If disaster recovery procedures are defined.							X
D.	If disaster recovery procedures are NOT defined.		X					
E.	If disaster recovery procedures have been disseminated to authorized personnel.							X
F.	If disaster recovery procedures have NOT been disseminated to authorized personnel.	X						

11. The desired outcome is that incident response and reporting procedures are in place and utilized. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If automated intrusion detection and reporting is implemented at the boundary layer.							X
B.	If automated intrusion detection and reporting is NOT implemented at the boundary layer.		X					
C.	If automated intrusion response has been implemented.							X
D.	If automated intrusion response has NOT been implemented.		X					
E.	If dynamic recovery and fail-over capabilities have been implemented.		X					
F.	If dynamic recovery and fail-over capabilities have NOT been implemented.						X	
G.	If penetration testing is periodically conducted.					X		
H.	If penetration testing is NOT periodically conducted.				X			

12. The desired outcome is that disaster recovery procedures have been put in place. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If dynamic recovery and fail-over capabilities have been implemented.							X
B.	If dynamic recovery and fail-over capabilities have NOT been implemented.			X				
C.	If backups of configuration files and firewall rule sets are maintained.							X
D.	If backups of configuration files and firewall rule sets are NOT maintained.	X						

13. The desired outcome is to have the system traffic flow be carefully monitored. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If the minimum throughput requirements have been defined.						X	
B.	If the minimum throughput requirements have NOT been defined.			X				
C.	If content scanning is effectively conducted at the boundary layer.						X	
D.	If content scanning is NOT effectively conducted at the boundary layer.		X					
E.	If mail filtering is conducted at the boundary layer.					X		
F.	If mail filtering is NOT conducted at the boundary layer.				X			
G.	If packet fragments are cued, reassembled, and inspected at the boundary layer.						X	
H.	If fragmented packets are NOT cued, reassembled, and inspected at the boundary layer.		X					

14. The desired outcome is that proactive management and auditing is conducted. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If active operational management techniques are employed.							X
B.	If active operational management techniques are NOT employed.	X						
C..	If rule sets are effectively documented and managed.							X
D.	If rule sets are NOT effectively documented and managed.	X						
E..	If logs are incorporated into the overall audit architecture.							X
F.	If logs are NOT incorporated into the overall audit architecture.		X					
G..	If trend analysis is conducted on audit and intrusion detection logs.							X
H.	If trend analysis is NOT conducted on audit and intrusion detection logs.		X					
I.	If patches and updates are kept current.					X		
J.	If patches and updates are NOT kept current.				X			

15. The desired outcome is that active, operational management techniques are employed. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If content scanning is effectively conducted at the boundary layer.					X		
B.	If content scanning is NOT effectively conducted at the boundary layer.		X					
C.	If mail filtering is conducted at the boundary layer.					X		X
D.	If mail filtering is NOT conducted at the boundary layer.				X			
E.	If packet fragments are cued, reassembled, and inspected at the boundary layer.						X	
F.	If fragmented packets are NOT cued, reassembled, and inspected at the boundary layer.		X					
E.	If automated data logging procedures have been put in place.						X	
F.	If automated data logging procedures have NOT been put in place.		X					

16. The desired outcome is to have procedures put in place that will support recovery from change. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If backups of configuration files and rule sets are maintained.							X
B.	If backups of configuration files and rule sets are NOT maintained.	X						
C.	If configuration criteria and standards are reviewed periodically.							X
D.	If configuration criteria and standards are NOT reviewed periodically.		X					
E.	If remote access control lists are maintained and closely monitored.						X	
F.	If remote access control lists are NOT maintained and closely monitored.	X						

17. The desired outcome is to have rule sets be completely documented and effectively managed. What is the effect on this outcome if the conditions below are met?

		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	NO IMPACT	Slightly Promotes	Moderately Promotes	Strongly Promotes
A.	If backups of configuration files and rule sets are maintained.							X
B.	If backups of configuration files and rule sets are NOT maintained.	X						
C.	If rules changes are evaluated to determine their security impact.							X
D.	If rules changes are NOT evaluated to determine their security impact.	X						
E.	If rules changes are fully justified and completely documented.						X	
F.	If rules changes are NOT fully justified and completely documented.		X					
G.	If rules sets are administered by authorized personnel only.						X	
H.	If rules sets are NOT administered strictly by authorized personnel.	X						

2. Node Value Survey

The following is a survey designed to collect data on the relative values of nodal values within the SIAM model. Completion of the survey should take approximately 45 minutes. This survey may be completed by typing directly into this document and emailing the file back to mailto:cpbrodhu@nps.navy.mil; or the survey may be completed in hard copy and faxed back to Major Brodhun, Code 32, NPGS, at (831) 656-3681 / DSN 878-4656.

COMMAND: Joint Information Operations Center

You will see desired outcomes listed below. Sets of potential conditions are listed in tables underneath each outcome. Place an "X" in the column to the right, which most accurately reflects the relative influence of each event on the desired outcome. This survey is NOT concerned with the existence or non-existence of the listed conditions in a specific implementation. Rather, this survey is addressing the RELATIVE TRUTH of the event.

INSTALLATION AND CONFIGURATION:

		Extremely Uncertain	Very Uncertain	Reasonably Uncertain	Slightly Uncertain	COMPLETELY UNCERTAIN	Slightly Certain	Reasonably Certain	Very Certain	Extremely Certain
1.	The manufacturer passwords have been changed.								X	
2.	The firewall(s) is/are physically secure.							X		
3.	The firewall(s) are installed by Authorized Personnel only.									X
4.	The "direction of flow" for each allowed and denied service has been determined and set.							X		

		Extremely Uncertain	Very Uncertain	Reasonably Uncertain	Slightly Uncertain	COMPLETELY UNCERTAIN	Slightly Certain	Reasonably Certain	Very Certain	Extremely Certain
5.	A split DNS has been implemented.								X	
6.	Specific services have been defined as "allowed."									X
7.	Specific services have been defined as "denied."									X
8.	The operating system supporting the firewall has been fully tested and patched (i.e., the OS is current).								X	
9.	The firewall(s) are supported by a secure network infrastructure.							X		
10.	The OS allows system configuration by users.								X	
11..	The OS feature set is known and well documented.							X		
12.	The IP Stack configurations are protected.								X	
13.	The firewall configurations allow for automated fail-over capabilities.					X				
14.	The infrastructure power is clean and protected within Enterprise boundaries.							X		
15.	The emergency power is available in case of an infrastructure failure.							X		
16.	The firewalls are installed in pairs to maintain a redundant architecture.				X					

ADMINISTRATION AND OPERATIONS:

		Extremely Uncertain	Very Uncertain	Reasonably Uncertain	Slightly Uncertain	COMPLETELY UNCERTAIN	Slightly Certain	Reasonably Certain	Very Certain	Extremely Certain
1.	The operational requirements of the organization (requirements levied on the system) have been well defined.							X		
2.	The minimum throughput requirements have been defined.					X				
3.	Content scanning is effectively conducted at the boundary layer.						X			
4.	Mail filtering is conducted at the boundary layer.					X				
5.	Packet fragments are cued, reassembled, and inspected at the boundary layer.					X				
6.	Automated data logging procedures have been put in place.							X		
7.	Penetration testing is periodically conducted.							X		
8.	Automated intrusion detection and reporting is implemented at the boundary layer.						X			
9.	Automated intrusion response has been implemented.					X				
10.	Dynamic recovery and fail-over capabilities have been implemented..				X					
11.	Backups of configuration files and firewall rule sets are maintained.							X		

		Extremely Uncertain	Very Uncertain	Reasonably Uncertain	Slightly Uncertain	COMPLETELY UNCERTAIN	Slightly Certain	Reasonably Certain	Very Certain	Extremely Certain
12.	Rules changes are evaluated to determine their security impact.						X			
13.	Rules changes are fully justified and completely documented.						X			
14.	Rules sets are administered by authorized personnel only.								X	
15.	Configuration criteria and standards are reviewed periodically.						X			
16.	Remote access control lists are maintained and closely monitored.						X			
17.	Patches and updates are kept current.							X		
18.	Trend analysis is conducted on audit and intrusion detection logs.						X			
19.	Logs are incorporated into the overall audit architecture.							X		

LIST OF REFERENCES

A. DOD REFERENCES

Buettner, R, Influence Modeling Workshop, August 6-7, 2001, Naval Postgraduate School.

Chairman of the Joint Chiefs of Staff, Information Assurance and Computer Network Defense, CJCSI 6510.01C, 2001

Department of Defense, Defense Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP), DoDI 8510.1, 2001

National Institute of Standards and Technology, Common Criteria for Information Technology Security Evaluation, v2.1, 1999.

National Security Telecommunications and Information Systems Security Committee (NSTISSC), NSTISS Instruction No. 4009, 1999.

United States Marine Corps, USMC NIPRNET Firewall Policy: Deployed and Garrison, 2000.

United States Navy, Fleet Firewall Policy, 1999.

United States Navy, Information Technology Standards Guidance (ITSG), v.99-1, 1999.

B. NON-DOD REFERENCES

Blanding, S., Secured Connections to External Networks, from Krause, M. and Tipton, H.F. Information Security Management Handbook, 4th ed., Volume 2, Auerbach Publications, 2000, ISBN: 0849308003.

Brenton, C., Mastering Network Security, Sybex Network Press, 1999, ISBN: 0782123430.

Brenton, C., et. al, Active Defense: A Comprehensive Guide to Network Security, Sybex, Inc., 2001, ISBN: 0782129161.

Cassidy, K., et. al., {The Concise Guide to} Enterprise Internetworking and Security, Que Corporation, 2001, ISBN: 0789724200.

Denning, D.E., Information Warfare and Security, ACM Press & Addison Wesley Longman, Inc., 1999, ISBN: 0201433036.

Denning, D.E., et. al., Internet Besieged: Countering Cyberspace Scofflaws, ACM Press & Addison Wesley Longman, Inc., 1998, ISBN: 0201308207.

Gollman, D., Computer Security, John Wiley & Sons, Ltd, 1999, ISBN: 0471978442.

Kabay, M.E., The NCSA Guide to Enterprise Security: Protecting Information Assets, The McGraw-Hill Companies, Inc., 1996, ISBN: 0700331472.

Krause, M. et. al., Handbook of Information Security Management 1999, CRC Press, Inc., 1999, ISBN: 0849399742.

Krause, M. et. al., Information Security Management Handbook, 4th ed., Auerbach Publications, 2000, ISBN: 0849398290.

Krause, M. et. al, Information Security Management Handbook, 4th ed., Volume 2, Auerbach Publications, 2000, ISBN: 0849308003.

Merkow, M.S., et. al.., The Complete Guide to Internet Security, AMACOM, 2000, ISBN: 081447070X.

Ogletree, T.W., Practical Firewalls, Que Corporation, 2000, ISBN: 0789724162.

Peltier, T.R., Information Security Policies and Procedures: A Practitioner’s Reference, Auerbach Publications, 1999, 0849399963.

Peltier, T.R., Information Security Risk Analysis, Auerbach Publications, 2001, ISBN: 0849308801.

Pfleeger, C.P., Security in Computing, 2nd ed., Prentice-Hall, Inc., 1997, ISBN: 0133374866.

Ranum, M., Internet Security Workshop, Networld+InterOp, 1996

Schneier, B., Secrets & Lies: Digital Security in a Networked World, John Wiley & Sons, Inc., 2000, ISBN: 0471253111.

Schultz, E., Firewalls: An Effective Solution for Internet Security, from Krause, M. and Tipton, H.F. Information Security Management Handbook, 4th ed., Volume 2, Auerbach Publications, 2000, ISBN: 0849308003.

Stallings, W., Network Security Essentials: Applications and Standards, Prentice-Hall, Inc., 2000, ISBN: 0130160938.

Strebe, M., et. al., Firewalls 24seven, Sybex, Inc., 2000, ISBN: 0782125298.

Zwicky, E.D., et. al., Building Internet Firewalls, 2nd ed., O’Reilly & Associates, Inc., 2000, ISBN: 1565928717.

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

Denning, D.E., and Denning, P.J., Internet Besieged: Countering Cyberspace Scofflaws, ACM Press & Addison Wesley Longman, Inc., 1998, ISBN: 0201308207.

Deputy Secretary of Defense, Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 6-8510 “Department of Defense Global Information Grid Information Assurance,” DoDCIOGPM 6-8510, 2000

Goncalves, M., Firewalls: A Complete Guide, The McGraw-Hill Companies, Inc., 2000, ISBN: 0071356398.

Goodyear, M., Enterprise System Architectures: Building Client/Server and Web-based Systems, Anderson Consulting & CRC Press, 2000, ISBN: 0849398363

Hatley, D., et al., Process for System Architecture and Requirements Engineering, Dorset House Publishing, 2000, ISBN: 0932633412

Kabay, M.E., The NCSA Guide to Enterprise Security: Protecting Information Assets, The McGraw-Hill Companies, Inc., 1996, ISBN: 0700331472.

Kaeo, M., Designing Network Security, Cisco Press & Macmillan Technical Publishing, 1999, ISBN: 1578700434.

Kaufmann, A., The Science of Decision Making: an Introduction to Praxeology, World University Library, 1968.

Linstone, H.A., Decision Making for Technology Executives: Using Multiple Perspectives to Improve Performance, Artech House Publishers, 1999, ISBN: 0890064032.

Maier, M.W., Rechtin, E., The Art of Systems Architecting, 2nd ed., CRC Press LLC, 2000, ISBN: 0849304407.

Merkow, M.S., and Breithaupt, J., The Complete Guide to Internet Security, AMACOM, 2000, ISBN: 081447070X.

Nichols, R.K., Ryan, D.J., Ryan, J.J.C.H, Defending Your Digital Assets Against Hackers, Crackers, Spies & Thieves, The McGraw-Hill Companies, Inc. / RSA Press, 2000, ISBN: 0072122854.

Office of Management and Budget, Memorandum 00-007, 2000

Ogletree, T.W., Practical Firewalls, Que Corporation, 2000, ISBN: 0789724162.

Peltier, T.R., Information Security Policies and Procedures: A Practitioner's Reference, Auerbach Publications, 1999, 0849399963.

Peltier, T.R., Information Security Risk Analysis, Auerbach Publications, 2001, ISBN: 0849308801.

Pipkin, D.L., Information Security: Protecting the Global Enterprise, Prentice Hall, PTR, 2000, 0130173231.

Schneier, B., Secrets & Lies: Digital Security in a Networked World, John Wiley & Sons, Inc., 2000, ISBN: 0471253111.

Stallings, W., Cryptography and Network Security: Principles and Practice, 2nd ed., Prentice-Hall, Inc., 1999, ISBN: 0138690170.

Tudor, J.K., Information Security Architecture: An Integrated Approach to Security in the Organization, Auerbach Publications, 2001, ISBN: 0849399882.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
8725 John J Kingman Road, Suite 0944
Fort Belvoir, VA 22060-6218

2. Dudley Knox Library
Naval Postgraduate School
411 Dyer Road
Monterey, CA 93943-5101

3. Mrs. Debra Filippi
HQMC, C4
TO: Navy Annex
Washington, DC 20380

4. Colonel Robert Baker, USMC
HQMC
C4, Plans and Policies Division
TO: Navy Annex
Washington, DC 20380

5. Mrs. Elaine Cassara
HQMC
C4IA Branch
TO: Navy Annex
Washington, DC 20380

6. Marine Corps Representative
Naval Postgraduate School
Monterey, California

7. Director, Training and Education, MCCDC, Code C46
Quantico, Virginia

8. Director, Marine Corps Research Center, MCCDC, Code C40RC
Quantico, Virginia

9. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
Camp Pendleton, California

10. Carl Siel
Space and Naval Warfare Systems Command
PMW 161
Building OT-1, Room 1024
4301 Pacific Highway
San Diego, CA 92110-3127

11. Captain Sheila McCoy, USN
DoN CIO

12. Commander, Naval Security Group Command
Naval Security Group Headquarters
9800 Savage Road
Suite 6585
Fort Meade, MD 20755-6585

13. Ms. Louise Davidson
N643
Presidential Tower 1
2511 South Jefferson Davis Highway
Arlington, VA 22202

Mr. William Dawson
Community CIO Office
Washington DC 20505

14. Ms. Deborah Phillips
Community Management Staff
Community CIO Office
Washington DC 20505

15. Captain James Newman, USN
N64
Presidential Tower 1
2511 South Jefferson Davis Highway
Arlington, VA 22202

16. Mr. Richard Hale
Defense Information Systems Agency, Suite 400
5600 Columbia Pike
Falls Church, VA 22041-3230

17. Ms. Barbara Flemming
Defense Information Systems Agency, Suite 400
5600 Columbia Pike
Falls Church, VA 22041-3230

18. Lieutenant Commander Raymond R. Buettner, USN
Information Warfare Department
Code IW
Naval Postgraduate School

19. Dr. William J. Haga
Graduate School of Business and Public Policy
Naval Postgraduate School

20. Dr. Cynthia E. Irvine
Computer Science Department
Code CS/IC
Naval Postgraduate School
Monterey, CA 93943